



Privacy, Data Protection and Copyright: Their Interaction in the Context of Electronic Copyright Management Systems

INSTITUTE FOR INFORMATION LAW, AMSTERDAM, JUNE 1998

Instituut voor Informatierecht (Institute for Information Law)
Rokin 84
1012 KX Amsterdam
Faculty of Law, University of Amsterdam
© Instituut voor Informatierecht 1998
ISBN 90-74243-15-0

Contents

1. Introduction	1
1.1 Preface	1
1.2 The Central Issue of this Report	1
1.3 First IMPRIMATUR Consensus Forum	2
1.4 Background to the Issue	2
1.4.1 The Nature of ECMS Operations	2
1.4.2 Affected Interests of the Data Subject	6
1.4.3 The Nature of Data Protection Laws.....	7
1.4.4 Other Important Legal Provisions.....	10
2. Application of Data Protection Laws to ECMS Operations	13
2.1 Personal Data	13
2.2 Data Controllers and Data Processors	15
2.3 Limits to Data Collection	16
2.3.1 Personal Data Generally.....	16
2.3.2 Especially Sensitive Data.....	19
2.4 Anonymity	22
2.5 Purpose Specification and Finality.....	23
2.5.1 Generally.....	23
2.5.2 Marketing.....	25
2.6 Orientation of Data Subjects.....	26
2.7 Security Measures	28
2.8 Transborder Data Flows	29
2.9 General Derogations.....	31
3. Application of Art 8 of the ECHR to ECMS Operations.....	33
4. Privacy-Enhancing Technologies	35
5. Copyright versus Privacy	37
5.1 Introductory Comments.....	37
5.2 Copyright vs. Privacy in the Analogue World.....	37
5.2.1 Copyright and Privacy do not Collide.....	38
5.2.2 Privacy Considerations in Copyright Law	40
5.3 Copyright vs. Privacy in the Digital World	43
5.3.1 Computer Programs and Databases	43
5.3.2 Copyright Directive Proposal.....	45
5.4 Technological Measures vs. Privacy	46
5.4.1 Monitoring	47
5.4.2 Blocking.....	48
5.5 Statutory Protection of Technological Measures	49
5.6 Statutory Protection of Copyright Management Information.....	52
5.7 Licenses	53
5.8 Maintaining the Balance.....	55
6. Conclusion	59
7. Legal SIG Workshop on Privacy, Data Protection, Copyright and ECMSs	61
7.1 Theme 1 – Copyright versus Privacy	62
7.2 Theme 2 – Data Protection in Electronic Transactions	68
7.3 Theme 3 – Do PETs make a difference?	70
Abbreviations.....	74
Bibliography	74

1. Introduction

1.1 Preface

This report is the fourth in a series of studies carried out for the IMPRIMATUR Consortium on possible legal problems associated with the design and operation of electronic copyright management systems.¹ The Institute for Information Law (IIL) of the University of Amsterdam has been engaged by the Consortium to carry out this series of studies. In the present study, the IIL has also relied upon expertise from the Norwegian Research Centre for Computers and Law (NRCCL) at the University of Oslo.

The authors of this report are Kamiel Koelman, associate researcher at the IIL, and Lee Bygrave, research fellow at the NRCCL. Line Coll has acted as research assistant for Lee Bygrave. Professors Jan Kabel (IIL) and Jon Bing (NRCCL) have supervised the study.

The views set forth in the report are primarily those of the authors and do not necessarily reflect the opinions of any of the IMPRIMATUR Consortium partners.

1.2 The Central Issue of this Report

This report investigates the way in which legal rules for the protection of privacy and of related interests can impinge upon the design and operation of an electronic copyright management system (ECMS) as exemplified by the IMPRIMATUR WP4 Business Model (Version 2.0).² The report does not canvass all rules for privacy protection; rather, it focuses upon rules that specifically regulate various stages in the processing (ie, collection, registration, storage, use and/or dissemination) of personal data in order to safeguard the privacy of the data subjects (ie, the persons to whom the data relate). By “personal data” is meant data that relate to, and permit identification of, an individual person. The main body of these legal rules is found in legislation that commonly goes under the nomenclature of data protection, at least in European jurisdictions. Accordingly, it is with the application of data protection legislation to ECMS operations that this report is mainly (though not exclusively) concerned.

The report is divided into two main parts, along with the Introduction and Conclusion. In brief, the first part of the report analyses the way in which the basic principles of privacy and data protection laws may apply to ECMS operations (see especially sections 2 and 3). The second part of the report analyses the various legal and technological balances that have been struck between the privacy interests of consumers and the interests of copyright holders, and considers the impact that an ECMS might have on these balances (see section 5).

¹ “IMPRIMATUR” stands for Intellectual Multimedia Property Rights Model and Terminology for Universal Reference. IMPRIMATUR is a project established by the Commission of the European Communities and co-ordinated by the UK Authors’ Licensing and Collecting Society (ALCS).

² Version 2.0 of the IMPRIMATUR Business Model is available at URL <http://www.imprimatur.alcs.co.uk/download.htm>.

It is important to note at the outset that this report does not attempt to grapple with issues of jurisdiction and choice-of-law. Neither does it consider in detail problems related to the enforceability of legal rules on privacy and data protection.

1.3 First IMPRIMATUR Consensus Forum

Privacy aspects of ECMS operations were previously considered at the First IMPRIMATUR Consensus Forum held in November 1996. There the following “Consensus Conclusions” were drawn:³

1. Privacy is a fundamental human right.
2. A general point of departure should be that a state of privacy is to be preferred rather than a state of no privacy.
3. “Privacy-Enhancing Technologies” (PETs) should be a design function in the IMPRIMATUR Business Model and “Identity Protectors” need to be built into any ECMS.
4. A reader should only be identified in a transaction if this is required by a specific law. When a reader is presented with a screen demanding personal data for further access, the fact that he or she refuses to go past that screen should not be recorded.
5. Support should be given to organisations within the “Rights Community” for the development of model codes of practice for the handling of personal data.
6. The IMPRIMATUR Business Model should include a Code of Conduct for Privacy in an ECMS. The Code should provide for administrative support to implementing PETs.
7. Participation in an ECMS by the creator of a copyrighted work should not be predicated upon the creator’s identity being revealed.

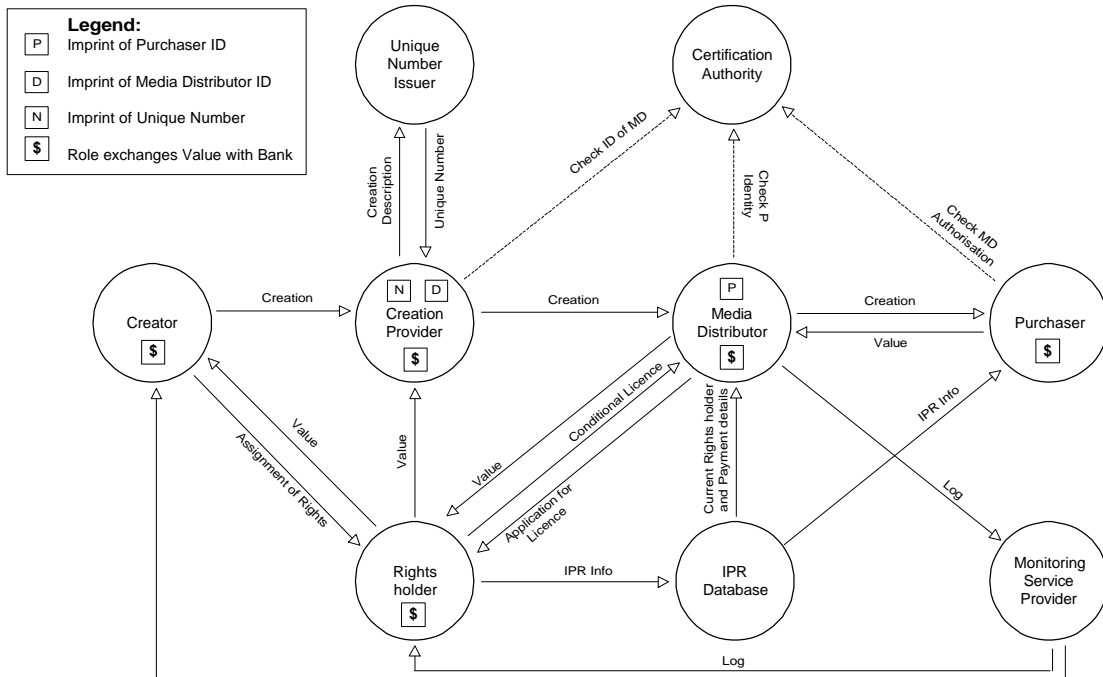
1.4 Background to the Issue

1.4.1 The Nature of ECMS Operations

Recent years have seen a marked growth in interest and opportunities for electronic commerce via distributed computer networks. The development of workable electronic copyright management systems is one part of this process. In a nutshell, these systems create a technological and organisational infrastructure that allows the creator of an original information product to enforce his/her/its copyright in the product when it is accessed on-line by other parties. An ECMS such as the IMPRIMATUR WP4 Business Model is predicated on the assumption that the process by which other parties acquire use of the copyrighted product is along the lines of a commercial contractual transaction; ie, these parties purchase from the creator, via intermediaries, an on-line disseminated copy of, and/or certain usage rights with respect to, the product.

³ See Proceedings of the First IMPRIMATUR Consensus Forum 1996: 85–90.

As intimated above, an ECMS typically involves the presence and interaction of one or more parties in addition to the creator, copyright-holder and purchaser. For example, the IMPRIMATUR WP4 Business Model (Version 2.0) involves the following actors and inter-relationships:



IMPRIMATUR Business Model (Version 2.0)

In brief, the role of the *creation provider* (CP) is analogous to that of a publisher; ie, he/she/it packages the original work into a marketable product. The role of the *media distributor* (MD) is that of a retailer; ie, he/she/it vends various kinds of rights with respect to usage of the product. The role of the *unique number issuer* (UNI) is analogous to the role of the issuer of ISBN codes; ie, it provides the CP with a unique number to insert in the product as microcode so that the product and its rights-holders can be subsequently identified for the purposes of royalty payments.⁴ The role of the *IPR database provider* is to store basic data on the legal status of the products marketed by the MD. These data concern the identity of each product and its current rights-holder. The main purpose of the database is to provide verification of a product's legal status to potential purchasers of a right with respect to usage of the product. As such, the IPR database is somewhat similar in content and function to a land title register. The role of the *monitoring service provider* (MSP) is to monitor, on behalf of creators/copyright-holders, what purchasers acquire from MDs. Finally, the *certification authority* (CA) is intended to assure any party to an ECMS operation of the authenticity of the other parties with whom he/she/it deals. Thus, the CA fulfils the role of trusted third party (TTP).

⁴ It is envisaged that this number will be in the form of an International Standard Work Code (ISWC), which, in turn, may be inserted in a Digital Object Identifier (DOI).

It is important to note that the IMPRIMATUR Business Model, along with most other electronic copyright management systems, are still in the process of being designed. Accordingly, there is some uncertainty about the parameters of their operation when they are finally put into practice on a widespread basis. More specifically, there is some uncertainty about the exact functions and inter-relationships of some of the above-described actors. It is quite possible, for instance, that the functions of some of these actors could be taken over by just one actor (eg, a CP could act as MD or MSP). Secondly, there is some uncertainty about the degree to which an ECMS like the IMPRIMATUR Business Model will be “fenced off” from other information systems. A pertinent question in this respect is to what extent and under what conditions data held within an ECMS will be accessible by external actors. Thirdly, the precise nature of the payment mechanisms to be employed in ECMS operations remains to be finalised. Fourthly, uncertainty exists over the amount and content of data that the various actors within an ECMS will register and further process.

It can be safely assumed, though, that at least some of the data processed by an ECMS will be person-related. One category of such data is the unique number (ISWC or the like), which enables identification of an information product’s creator, author, editor, etc. This category of data will flow through most points of an ECMS. A second category of personal data is data relating to purchasers. These data will be primarily registered by MDs and stored in their sales logs. There is another category of personal data which might be registered: these are data relating to browsers (ie, persons who inspect or sample an information product without purchasing a particular right with respect to it). Like purchaser-related data, these data will be primarily registered and stored – if at all – by MDs.

Of the above three categories of personal data, the first-mentioned raises few privacy problems for the data subjects, relative to the other two data categories. The creator, author, editor, etc of copyrighted material must expect that this material, and their involvement with it, will receive considerable publicity. The same cannot be said for the purchaser and browser, however. Accordingly, this report focuses on the privacy rights of the latter two actors. It is important to note, though, that the first-mentioned category of data may still qualify for protection under some data protection laws and other legal rules on privacy.⁵

The amount and content of purchaser- and browser-related data which are registered in an ECMS, together with the manner in which these data are used and disseminated, will depend on a range of factors. One set of factors are legal. For example, data protection laws (as shown further below) set limits on the extent to which personal data may be registered and further processed.

Another set of factors are economic. For example, a MD might desire to register as much purchaser- and browser-related data as possible, in order to create detailed customer

⁵ However, some such laws currently exempt this sort of data from their protection: see, eg, s 2(1)(c) of the Netherlands’ Act of 1988 on Protection of Privacy in Connection with Personal Data Files; Art 3(2)(3) of the Belgian Act of 1992 on Protection of Personal Privacy in Relation to the Processing of Personal Data.

profiles that can be subsequently used (by the MD itself or by others) for cross-selling and other marketing purposes. Concomitantly, the MD could make purchases and browsing contingent upon the purchaser and browser disclosing a great detail of information about themselves. On the other hand, a MD might want to reduce its registration and usage of purchaser- and browser-related data in order to attract the custom of those who are seriously concerned about possible infringements of their privacy.

A third set of factors are technical-organisational. For instance, an entity operating as MD might sell a multiplicity of goods and services (eg, food products, travel tickets, etc) in addition to usage rights to copyrighted information. If a purchaser or browser has contact with the MD also in respect of these other goods and services, the MD will end up having a great deal of information about the purchaser or browser's personal preferences. Concomitantly, a one-off sales transaction or "shop visit" is likely to involve registration of less data on the purchaser or browser than in the case of frequent or regular transactions pursuant to some form of service subscription. To take another example, the amount of browser-related data which are registered by a MD will depend on, *inter alia*, the extent to which the latter's server utilises mechanisms for automatically registering such data (eg, as "cookies").⁶

This third set of factors, however, will tend to be ultimately derivative of the first two sets (ie, legal and economic factors), with one *current* exception: at present, it is usually not possible to visit an Internet server without the browser software automatically revealing certain data to the server. These data are typically the network identity (hostname and IP address) of the browser's machine, the URL of the last page visited by the browser before coming to the present server, and whatever cookies that are stored on the browser's computer.⁷ Whether or not such data can be said to be "personal" pursuant to data protection laws is an issue dealt with in section 2.1 below.

At the same time, sight should not be lost of the fact that services are springing up which allow for the use of anonymising servers as intermediaries for browsing and/or purchasing transactions on the Internet.⁸ Nevertheless, such servers will usually not guarantee full transactional anonymity as they will also record certain details about a browser's/purchaser's Internet activities – details which could be accessed by others under exceptional circumstances.⁹ It is also an open question as to whether or not a MD in an ECMS would be willing to allow use of anonymising servers by purchasers or browsers.

In any case, anonymising servers highlight the fact that there are a number of technical and organisational tools being developed in order to safeguard the privacy and related interests of persons using the Internet. These tools often go under the nomenclature of

⁶ In brief, "cookies" are transactional data about a browser's Internet activity which are automatically stored by an Internet server on the browser's computer. See further Mayer-Schönberger 1997.

⁷ Greenleaf 1996a: 91–92.

⁸ See, eg, URL <http://www.anonymizer.com/faq.html>.

⁹ *Ibid.*

“privacy-enhancing technologies” or “PETs”. The application of such tools to ECMS operations is an issue that this report addresses in section 4 below.

1.4.2 Affected Interests of the Data Subject

The registration and/or further processing of purchaser- and browser-related data in an ECMS may impinge on a multiplicity of interests of the data subjects. The most important of these interests for the purposes of this report may be summed up in terms of privacy, autonomy and integrity. Each of these concepts are nebulous and often used in haphazard fashion.

For present purposes, the concept of privacy denotes a state of limited accessibility consisting of three elements: secrecy – “the extent to which we are known to others”; solitude – “the extent to which others have physical access to us”; and anonymity – “the extent to which we are the subject of others’ attention”.¹⁰ It should be emphasised that privacy here is not delimited to apply only to those aspects of persons’ lives that are considered as sensitive or intimate.

The concept of autonomy denotes self-determination; ie, a person’s capacity to live his/her life in accordance with his/her own wishes (including, of course, the capacity to use goods as he/she sees fit). In the context of this report, it is a person’s self-determination on the informational plane that is of main importance. Many scholars (eg, Westin 1967; Miller 1971) define privacy in terms of a person’s ability to control the flow of information about him-/herself to others; in this report, such informational self-determination is viewed as a precondition for, and result of, privacy (ie, limited accessibility).

As for the concept of integrity, this is used here to denote “a person’s state of intact, harmonious functionality based on other persons’ respect for him/her”.¹¹ A breach of integrity will therefore involve disruption of this functionality by the disrespectful behaviour of other persons.

In the context of an ECMS, a purchaser and browser’s privacy will be diminished by the mere registration by a MD of data that can be linked back to them. Their autonomy will also be diminished insofar as the registration occurs without their consent or knowledge, or insofar as the registration causes them to behave along lines determined primarily by the MD or another ECMS actor. And their integrity will be detrimentally affected insofar as the registration or subsequent use of the data does not conform with their expectations of what is reasonable. For example, many persons are likely to view the non-consensual or surreptitious processing of data on them by others as integrity-abusive.

The mere registration of data will not be the only activity that can diminish the privacy, autonomy and/or integrity of data subjects. Other stages in the data-processing cycle will potentially affect these interests as well. Especially problematic will be the use, re-use

¹⁰ Gavison 1980: 428–436.

¹¹ Bygrave 1998a: 42.

and/or dissemination of data for secondary purposes; ie, purposes that vary from the purposes for which the data were originally collected. A typical example here is when personal data originally registered in order to ensure non-repudiation of a particular transaction are subsequently used for the purposes of cross-selling or other marketing of products *vis-à-vis* the data subjects. Such “re-purposing” of data will be particularly problematic if it occurs without the data subjects’ prior consent or if it falls outside the data subjects’ reasonable expectations. It will also be problematic, not just for the data subjects but also the data user, if it involves the application of data for purposes for which the data are not suited.

The latter point highlights the fact that safeguarding the privacy, autonomy and integrity interests of data subjects will not always conflict with the interests of data users. Moreover, people’s readiness to enter into electronic commerce as consumers (or “prosumers”) will be largely contingent upon the degree to which they feel confident that their privacy, autonomy and integrity interests will be respected by the other actors in the market.¹² Indeed, an increasingly major task of data protection laws and related measures is precisely that of building up such confidence.¹³

Arguably, the most important point that should be emphasised here is that the development of electronic copyright management systems has the *potential* to impinge on the privacy, autonomy and integrity interests of information consumers to an unprecedented degree. In other words, such systems could facilitate the monitoring of what people privately read, listen to, or view, in a manner that is both more fine-grained and automated than previously practised. This surveillance potential may not only weaken the privacy of information consumers but also function as a form for thought control, weighing down citizens with “the subtle, imponderable pressures of the orthodox”,¹⁴ and thereby inhibiting the expression of non-conformist opinions and preferences. In short, an ECMS could function as a kind of digital Panopticon. The attendant, long-term implications of this for the vitality of pluralist, democratic society are obvious.

1.4.3 The Nature of Data Protection Laws

Data protection laws emerged in the 1970s in response to a congeries of public fears about the potentially privacy-invasive consequences of computer technology. Well over twenty countries have now enacted such laws. Most of these countries are European. Important countries outside Europe (notably, the USA, Canada, Japan, Australia and New Zealand) have also data protection legislation in place, though this is often less

¹² Samarijiva 1997: 282ff.

¹³ See, eg, Canadian Task Force on Electronic Commerce 1998: 6 (“In an environment where over half of Canadians agree that the information highway is reducing the level of privacy in Canada, ensuring consumer confidence is key to securing growth in the Canadian information economy. Legislation that establishes a set of common rules for the protection of personal information will help to build consumer confidence ...”).

¹⁴ The phrase is taken from the concurring opinion of Justice Douglas in *US v Rumely*, 345 US 41 (1953), 58.

comprehensive and stringent than the European legislation.¹⁵ In addition to national data protection laws, a range of data protection instruments have been adopted at an international level. The most influential of these have been worked out under the auspices of the European Union (EU), Council of Europe (CoE) and Organisation for Economic Co-operation and Development (OECD). These instruments are:

- (i) the European Union's *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*,¹⁶ adopted by the European Parliament and the Council on 24.10.1995;
- (ii) the Council of Europe's *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*,¹⁷ adopted by the CoE Committee of Ministers on 28.1.1981; and
- (iii) the OECD's *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*,¹⁸ adopted by the OECD Council on 23.9.1980.

The United Nations (UN) has also issued *Guidelines Concerning Computerized Personal Data Files*,¹⁹ adopted by the UN General Assembly on 4.12.1990. These guidelines, however, have received relatively little attention.

Each of the above international instruments are of general ambit. They have been supplemented by a range of instruments dealing with aspects of data processing within specified sectors. Some of these sectoral instruments have been drafted and adopted by the CoE as recommendations. Of particular relevance for this report are: *Recommendation No R (85) 20 on the protection of personal data used for the purposes of direct marketing*, adopted 25.10.1985; *Recommendation No R 90 (19) on the protection of personal data used for payment and other related operations*, adopted 13.9.1990; and *Recommendation No R (95) 4 on the protection of personal data in the area of telecommunications services, with particular reference to telephone services*, adopted 7.2.1995. Another sectoral instrument of particular relevance for this report is the EU's *Directive on the processing of personal data and the protection of privacy in the telecommunications sector*.²⁰ Also of relevance are various sets of guidelines dealing specifically with the processing of personal information over the Internet.²¹

At a national level, special mention must be made of Germany's *Teleservices Data Protection Act* of 1997.²² This is, to our knowledge, the first law to deal specifically with

¹⁵ See below for examples.

¹⁶ Directive 95/46/EC (OJ No L 281, 23.11.1995, 31) – hereinafter termed “EU Data Protection Directive” or “DPD”.

¹⁷ ETS No 108 – hereinafter termed “CoE Data Protection Convention”. The Convention entered into force on 1.10.1985.

¹⁸ Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (Paris: OECD, 1980).

¹⁹ Guidelines Concerning Computerized Personal Data Files (Doc E/CN.4/1990/72, 20.2.1990).

²⁰ Directive 97/66/EC (OJ No L 024, 30.1.1998, 1) – hereinafter termed “EU ISDN Directive”.

²¹ See especially Data Protection Working Party 1997b and Information Infrastructure Task Force 1995.

²² In force as of 1.8.1997. The Act was passed as part of a federal legislative package “to Regulate the Conditions for Information and Communications Services”. An English translation of the entire legislative package is available at URL <http://www.iid.de/iukdg/iukdge.html>. For the German version, see URL <http://www.iid.de/rahmen/iukdgk.html>.

data protection issues in an Internet context. It can be expected to exert considerable influence on other countries' legislative activity in the field.

The central rules of data protection laws are built up around the following set of principles:

- (i) personal data should be gathered by fair and lawful means (hereinafter termed "fair collection principle");
- (ii) the amount of personal data gathered should be limited to what is necessary to achieve the purpose(s) of gathering the data (hereinafter termed "minimality principle");
- (iii) personal data should be gathered for specified and lawful purposes and not processed in ways that are incompatible with those purposes (hereinafter termed "purpose specification principle");
- (iv) use of personal data for purposes other than those specified should occur only with the consent of the data subject or with legal authority (hereinafter termed "use limitation principle");
- (v) personal data should be accurate, complete and relevant in relation to the purposes for which they are processed (hereinafter termed "data quality principle");
- (vi) security measures should be implemented to protect personal data from unintended or unauthorised disclosure, destruction or modification (hereinafter termed "security principle");
- (vii) data subjects should be informed of, and given access to, data on them held by others, and be able to rectify these data if inaccurate or misleading (hereinafter termed "individual participation principle").
- (viii) parties responsible for processing data on other persons should be accountable for complying with the above principles (hereinafter termed "accountability principle").

These are not the only principles manifest in data protection laws but they are the main ones. Another principle is worth noting too; this is that fully automated evaluations of a person's character should not be used to reach decisions that significantly impinge upon the person's interests. This principle is not yet manifest in the majority of data protection laws but will gain more prominence on account of it being embodied in Art 15 of the EU Data Protection Directive.²³

While data protection laws enjoy common ground in terms of most of the above principles, they presently differ in terms of their ambit. Some countries' laws only apply to data processing by public sector bodies,²⁴ while most other countries' laws, and all of the international data protection laws, apply also to data processing by private sector bodies. Some countries' laws only apply to computerised/automated processing of data,²⁵ while most other countries' laws apply also to non-automated processing. Some countries' laws give express protection for data relating to legal/juridical persons (ie,

²³ The principle has its legal origins in s 2 of France's Act of 1978 on Data Processing, Data Files and Individual Liberties.

²⁴ See, eg, the US federal Privacy Act of 1974, Canada's federal Privacy Act of 1982 and Australia's federal Privacy Act of 1988.

²⁵ See, eg, Sweden's Data Act of 1973 and the UK's Data Protection Act of 1984.

corporations and the like)²⁶ – in addition to data relating to individual natural/physical persons – while most other countries’ laws expressly protect only the latter data.

Differences occur also with respect to the regulatory regimes established pursuant to each law. For instance, while most countries’ laws provide for the establishment of a special independent agency (hereinafter termed “data protection authority”) to oversee the laws’ implementation, this is not the case with respect to the laws of the USA and Japan. To take another example, while most countries’ laws contain express restrictions on the flow of personal data to other countries that lack adequate data protection safeguards, some countries’ laws do not.²⁷ To take a third example, while some countries’ laws do not allow certain data-processing operations to commence without the operations first being checked and licensed by the relevant data protection authority,²⁸ other countries’ laws permit all or most operations to commence simply on the data protection authority first being notified of the operations.²⁹

In this report, the main point of departure for legal analysis will be the international instruments on data protection set out above, in particular the EU Data Protection Directive. The latter instrument is likely to exercise the greatest influence on new data protection initiatives, both in and outside the EU. Member States of the EU have been given, with a few exceptions, until 24.10.1998 to bring their respective legal systems into conformity with the provisions of the Directive (see Art 32(1) of the latter). If – as is likely – the Directive is incorporated into the 1992 Agreement on the European Economic Area (EEA), then countries that are not members of the EU but party to the EEA Agreement (ie, Norway, Iceland and Liechtenstein) will also become legally bound to bring their respective laws into conformity with the Directive. In addition, the Directive is likely to exercise some political and legal influence over other countries outside the EU, not least because the Directive, with some exceptions, prohibits the transfer of personal data to these countries if they do not provide “adequate” levels of data protection (see Art 25(1), discussed below in section 2.8).

1.4.4 Other Important Legal Provisions

The formal normative roots of data protection laws lie mainly in the right to privacy set down in international catalogues of fundamental human rights, particularly Art 17 of the 1966 *International Covenant on Civil and Political Rights* (ICCPR) and Art 8 of the 1950 *European Convention for the Protection of Human Rights and Fundamental Freedoms*

²⁶ See Norway’s Personal Data Registers Act of 1978, Iceland’s Act of 1989 on the Registration and Handling of Personal Data, Austria’s Data Protection Act of 1978, Luxembourg’s Nominal Data (Automatic Processing) Act of 1979, Switzerland’s Federal Data Protection Act of 1988, Italy’s Act of 1996 on the Protection of Individuals and Other Subjects with regard to the Processing of Personal Data, and Denmark’s Private Registers Act of 1978.

²⁷ See, eg, the US federal Privacy Act of 1974 and Australia’s federal Privacy Act of 1988.

²⁸ See, eg, Norway’s Personal Data Registers Act of 1978 and Sweden’s Data Act of 1973.

²⁹ See, eg, Switzerland’s federal Data Protection Act of 1993 and Italy’s Act of 1996 on the protection of individuals and other subjects with regard to the processing of personal data.

(ECHR). Indeed, this is expressly recognised in many of the data protection instruments themselves.³⁰

Article 17 of the ICCPR provides:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks upon his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.

Article 8 of the ECHR provides:

1. Everyone has the right to respect for his private and family life, his home and correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Both provisions have been interpreted as capable of addressing data protection issues.³¹ In prescriptive terms, however, the case law developed pursuant to these provisions adds nothing, so far, to what is found in ordinary data protection instruments. In other words, while these provisions operate, to some extent, as data protection instruments in their own right, they give little guidance on the legal requirements for processing personal data.

The most extensive relevant case law has been developed by the European Court of Human Rights pursuant to Art 8 of the ECHR, but even this case law is fairly meagre, particularly with respect to the data-processing practices of private sector bodies. Indeed, the Court has yet to have treated a case pursuant to Art 8 which involves the latter data-processing practices. Nevertheless, it is highly unlikely that such practices will be held as falling outside the protective scope of Art 8, given that CoE Member States, both nationally and internationally,³² apply data protection rules to both the private and public sectors. It is also important to note that Art 17 of the ICCPR has been interpreted by the UN Human Rights Committee as requiring implementation of basic data protection guarantees in both sectors.³³ Thus, the processing of purchaser-/browser-related data in the context of ECMS operations has the potential to impinge on purchasers'/browsers' rights laid down in Art 8 of the ECHR and Art 17 of the ICCPR – in addition to impinging on their rights set down in laws dealing specifically with data protection. A short analysis of the way in which Art 8 case law might apply to ECMS operations is given in section 3 below.

It should also be noted that the constitutions of many countries contain provisions that require, expressly or impliedly, implementation of basic data protection principles. Arguably the most solid constitutional underpinning for data protection in a European

³⁰ See, eg, Art 1 and recital 10 of the EU Data Protection Directive and Art 1 of the CoE Data Protection Convention.

³¹ For a comprehensive analysis, see Bygrave 1998b.

³² See, eg, the CoE Data Protection Convention.

³³ See the Committee's General Comment 16, issued 23.3.1988 (UN Doc A/43/40, 181–183).

country is provided by the Federal Republic of Germany's *Basic Law (Grundgesetz)* of 1949. The Basic Law contains several provisions which have been held to relate to data protection. Article 1(1) provides that "[t]he dignity of man shall be inviolable", while Art 2(1) states that "[e]veryone shall have the right to the free development of his personality in so far as he does not violate the rights of others or offend against the constitutional order or against morality". Article 10 states that "[p]rivacy of letters, posts and telecommunications shall be inviolable", and Art 13 upholds the inviolability of the home. In a famous and influential decision of 15.12.1983, the German Federal Constitutional Court (*Bundesverfassungsgericht*) held that Articles 1 and 2 of the Basic Law provide individuals with a right to "informational self-determination" ("informationelle Selbstbestimmung"); ie, a right for the individual "to decide for him-/herself ... when and within what limits facts about his/her personal life shall be publicly disclosed".³⁴ The Court went on to hold that this right will be infringed if personal data are not processed in accordance with basic data protection principles, including that of purpose specification ("Zweckbindung").

³⁴ BVerfGE 1983/65: 1, 42–43 (*Volkzählungsgesetz*).

2. Application of Data Protection Laws to ECMS Operations

In the following, we do not address the totality of ways in which data protection laws can be expected to apply to ECMS operations; rather, we focus on what we consider to be the most important points of application. These points concern the scope of the concept of “personal data” in data protection laws (see section 2.1), who is primarily responsible for complying with these laws’ obligations (see section 2.2), and the basic conditions these laws set down for the processing of personal data (see sections 2.3 to 2.9).

2.1 Personal Data

As intimated above, the ambit of data protection laws is restricted to situations in which *personal* data are processed. In other words, the design and operation of an ECMS may be affected by data protection laws only insofar as the ECMS processes such data. The concept of personal data is usually defined by the laws in a broad and flexible manner. For instance, Art 2(a) of the EU Data Protection Directive (DPD) defines “personal data” as

any information relating to an identified or identifiable natural person (“data subject”); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.³⁵

Domestic data protection laws contain broadly similar definitions of “personal data” or “personal information”. The focus of these definitions on the criterion of direct or indirect identifiability (ie, on the potential of information to enable identification of a person) makes them capable in theory of embracing a great deal of data that *prima facie* have little direct relationship to a particular person. Thus, data may be “personal” even if they allow a person to be identified only in combination with other (auxiliary) data.³⁶

At the same time, though, certain limitations are usually read into the identifiability criterion such that identification must be possible using methods that do not involve an unreasonably large amount of time, expense and labour. Paragraph 28 of the Explanatory Report for the CoE Data Protection Convention states that an “identifiable person” is one “who can be *easily* identified: it does not cover identification of persons by means of *very sophisticated* methods” (emphasis added). Subsequent elaborations of the identifiability criterion in relation to the CoE’s various sectoral recommendations on data protection introduce the factors of reasonableness, time, cost and resources. For example, para 1.2 of Rec No R (85) 20 on the protection of personal data used for the purposes of direct marketing, states, *inter alia*, that “[a]n individual shall not be regarded as “identifiable” if the identification requires an unreasonable amount of time, cost and manpower”. Recital 26

³⁵ Recital 14 in the Directive’s preamble makes clear that this definition also encompasses sound and image data on natural persons.

³⁶ See, eg, European Commission 1992: 9 (“A person may be identified directly by name or indirectly by a telephone number, a car registration number, a social security number, a passport number or by a combination of significant criteria which allows him to be recognized by narrowing down the group to which he belongs (age, occupation, place of residence, etc)”).

of the DPD lays down what appears to be a broader and more flexible criterion for identifiability: “to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person”. Nevertheless, the Directive’s criterion is probably similar in effect to the criteria read into the above CoE instruments.³⁷ National laws which expressly qualify degree of identifiability also employ similar criteria, either directly³⁸ or indirectly.³⁹

Usually, data must be capable of being linked to a *particular individual* person before they are to be regarded as “personal” pursuant to data protection laws. Thus, data which can only be linked to an aggregate of persons will normally fall outside the ambit of such laws. Some countries, though, have data protection legislation that expressly covers data on collective entities such as corporations, partnerships and citizen initiative groups;⁴⁰ nevertheless, such data are only covered if they can be linked back to one particular entity as opposed to a multiplicity of entities.

From the above, it can be seen that the legal threshold for what amounts to personal data is low. It is likely, therefore, that an ECMS such as the IMPRIMATUR WP4 Business Model will involve the processing of personal data, including data that can be linked to specific purchasers and browsers. However, exactly which types of data will be regarded as “personal” is a question of fact that is impossible to answer conclusively at present. Of greatest interest in this regard is the extent to which e-mail addresses and/or machine addresses (ie, IP numbers and domain names) can properly be said to amount to personal data. The answer to this issue will depend on the ease/probability of linking such addresses to a specific person. If, for instance, there is a readily accessible directory listing one particular person against one particular address, the latter is likely to be seen as personal data.⁴¹ This will not be the case, however, if a multiplicity of persons are registered against that address. At the same time, though, the possibility of a multiplicity of persons sharing a machine with an address registered in the name of only one person will not disqualify that machine address from being treated as personal data. Many

³⁷ Note too recital 27 of the DPD with respect to ease of access to personal data in “personal data filing systems”: “the content of a filing system must be structured according to specific criteria relating to individuals allowing *easy* access to the personal data” (emphasis added).

³⁸ See, eg, Art 2(a) of Portugal’s Act of 1991 on Protection of Personal Data with Regard to Automatic Processing (“an individual will be regarded as identifiable if the identification does not require an unreasonable amount of time or cost”); and s 2(2) of Finland’s Personal Data File Act of 1987 (defining “personal data file” as “a set of data ... from which data on a certain person can be found easily and without unreasonable expense”).

³⁹ For instance, a criterion of proportionality is read in to the identification process envisaged by s 3(1) of the FRG’s Federal Data Protection Act of 1990 so as to exclude cases where identification is only possible through a data controller making an effort that is “disproportionate” in relation to his/her/its “normal” means and activities. This criterion of proportionality is derived from s 3(7) of the Act which defines “depersonalized data” as information which “can no longer be attributed to ... [an identified or identifiable natural person] or only with a disproportionately great expenditure of time, money and labour”.

⁴⁰ See, eg, s 3(2) of Austria’s Data Protection Act of 1978 and Art 1(2)(c) of Italy’s Act of 1996 on the protection of individuals and other subjects with regard to the processing of personal data. Note that the EU Directive does not address the issue of whether or not data on collective entities are to be protected; hence, each EU Member State is able to arrive at its own decision on the appropriateness of such protection.

⁴¹ See also Greenleaf 1996b: 114–115.

numbers (eg, car registration and telephone numbers) which are formally registered against the name of one specific person are treated as personal data even if the objects to which they directly attach are occasionally or regularly used by other persons.

2.2 Data Controllers and Data Processors

Primary responsibility for observing the rules laid down in data protection laws is given to those actors that control the means and purposes of the processing of data on other persons. In the nomenclature of the DPD, such actors are termed “controllers” (hereinafter also called “data controllers”). Article 2(d) of the Directive defines a “controller” as the “natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data”.

Four points should be noted with respect to this definition. First, it envisages the possibility of there being more than one controller per data-processing operation (ie, control can be shared). Secondly, a controller need not be in possession of the personal data concerned.⁴² Thirdly, who is controller can change from one data-processing operation to another, even within one information system. Fourthly, what is decisive for determining who is controller is not the formal allocation of control responsibilities as set down in, say, contractual provisions, but the *factual* exercise of control. Thus, if a legal provision allocates control responsibilities to one party but the control is actually exercised by another party, it is the latter who must be regarded as the controller for the purposes of the DPD.

In the context of an electronic communications network, recital 47 in the preamble to the DPD indicates that, for the purposes of the Directive, the person or organisation providing the transmission services is normally not to be regarded as the controller of personal data contained in a transmitted message; the controller will instead be the person or organisation “from whom the message originates”. However, transmission service providers “will normally be considered controllers in respect of the processing of the additional personal data necessary for the service”.

A controller is to be distinguished from what the DPD terms a “processor”. The latter is defined in Art 2(e) of the Directive as a person or organisation engaged in processing personal data “on behalf of” a data controller. Under the Directive, controllers must ensure, through appropriate contractual or other arrangements, that processors carry out their tasks in accordance with the laws that are enacted pursuant to the Directive. Liability for a processor’s non-compliance with these laws is put on the shoulders of the controllers. Accordingly, for the purposes of ECMS operations, it is more crucial to determine which actors are controllers than determining which actors are processors.

⁴² See also Terwangne & Louveaux 1997: 236 (“There is no requirement that the controller be in actual possession of the data; it is the concept of control that is important”).

As noted in the Introduction, uncertainty still reigns over the exact powers and functions of each of the actors in an ECMS such as the IMPRIMATUR WP4 Business Model. A pertinent question here concerns which actors are to be regarded as controllers with respect to registration and other processing of purchaser-related data. Several possibilities exist. For instance, it could be that the CP and/or copyright-holder solely determine(s) the means and purposes of the registration of all (or some) of these data, with the MD and MSP acting simply as processors in this regard. Alternatively, either one of the latter actors will also be a controller with respect to those data if he/she/it co-determines the means and purposes of the data processing. As noted above, what will be decisive for determining who is controller with respect to a given data-processing operation is not the formal allocation of control responsibilities pursuant to contract, but the *factual* exercise of control.

Any of the above ECMS actors will be *sole* controllers with respect to processing operations of which they alone determine the means and purposes. It is not unlikely, for example, that the MD will be sole controller in relation to registration and further processing of *browser*-related data, given that such data are not of direct relevance for the interests of the CP, copyright-holder, MSP or CA.

2.3 Limits to Data Collection

2.3.1 Personal Data Generally

As indicated in the Introduction, a core principle of data protection laws is that personal data should be gathered by fair and lawful means. This principle is set out expressly in Art 6(1)(a) of the DPD. “Lawful” is a criterion which is relatively self-explanatory. As for the criterion of “fair”, this is not specifically defined in the Directive and its exact ambit is uncertain. One can safely assume, though, that fairness embraces a requirement that personal data not be collected in a surreptitious or overly intrusive manner.⁴³

The DPD prohibits the collection and further processing of personal data unless the processing satisfies specified conditions. These are laid down in Art 7 as follows:

- (a) the data subject has unambiguously given his consent [to the processing], or
- (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract, or
- (c) processing is necessary for compliance with a legal obligation to which the controller is subject, or
- (d) processing is necessary in order to protect the vital interests of the data subject, or
- (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed, or
- f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection under Article 1(1).

Of these conditions, paras (a), (b), (c) and (f) are pertinent to the operation of an ECMS.

⁴³ See also Terwangne & Louveaux 1997: 239.

Regarding para (a), this must be read in light of Art 2(h), which defines “the data subject’s consent” as “any freely given specific and informed indication of his wishes, by which the data subject signifies his agreement to personal data relating to him being processed.” From this definition, it appears that consent need not be in writing. However, the express registration of consent on paper or electronic medium will aid in fulfilling the requirement in Art 7(a) that consent be “unambiguous”. Arguably, the latter requirement will be met even if consent is not explicit (see below), but the data subject’s actions must leave no doubt that he/she has given consent.

In the context of an ECMS, the simple fact that a purchaser takes the initiative to enter into a transaction with the MD could be seen as a manifestation of consent to the MD’s registration of at least some data on the purchaser. However, this consent will only extend to the registration practices which the purchaser could reasonably expect or about which the purchaser is notified by the MD. Given the Directive’s concern to ensure that data processing is carried out in a manner that is *fair* to the interests of data subjects,⁴⁴ notification of the purchaser will have to be done in such a way as to help ensure such fairness. Thus, notification will arguably need to occur *prior* to the purchase transaction taking place (ie, during the browsing phase), and it will need to involve *active steps* on the part of the controller (ie, through the latter creating screen-icons that can reasonably be said to catch the attention of potential purchasers).⁴⁵

The same applies with respect to browsers. If a person decides to browse a MD’s server *after* being made aware (eg, by an appropriately formatted notice on the first server page visited) that the MD will register certain data on the person’s browsing activity, the person should be taken as impliedly (and unambiguously) consenting to such registration.

However, the registration of the fact that a person accesses a MD’s server – without the person necessarily going on to browse through the server’s various pages – is not justifiable under para (a), if the person is not given an opportunity to consent to that registration. Hence, if a MD’s server operates with a mechanism for automatically creating and setting cookies at the time the server is first accessed, and if the cookies constitute personal data (see section 2.1 above), the mechanism will fall outside the bounds of para (a). Indeed, in the context of ECMS operations, it is hard to see that such a cookies mechanism will meet any of the other conditions in Art 7, except possibly those laid down in paras (b) and (f).⁴⁶

It goes without saying that if the processor or controller processes browser- /purchaser-related data along parameters that differ fundamentally from those parameters about which the browser/purchaser was first notified and to which the latter agreed (implicitly or explicitly), the processing will be unlawful unless consent is given anew or the processing meets the other conditions laid down in Art 7.

⁴⁴ See Art 6(1)(a) set out at the beginning of this section. See also Arts 10 and 11(1) set out in section 2.6 below.

⁴⁵ See also Terwangne & Louveaux 1997: 239 & 241.

⁴⁶ Note also § 3(5) of Germany’s Teleservices Data Protection Act, set out in section 2.6 below.

The condition set out in Art 7(b) will often be met with respect to the processing of purchaser-related data in the context of an ECMS, given that there will exist a contract between the purchaser and the MD. The condition may also be satisfied with respect to the processing of browser-related data insofar as the processing is “in order to take steps at the request of the data subject prior to entering into a contract”. The main point of concern is to determine which data processing is “necessary” in both cases. Of particular interest here will be determining the extent to which Art 7(b) can properly be used as justification for the monitoring of purchasers’ private activities after a contract is entered into, so as to check compliance with the contract.

The necessity criterion in Art 7(b) should be read as embracing two overlapping requirements: (1) that the processing corresponds to a pressing social or commercial need; and (2) that the processing is proportionate to the aim of the contract.⁴⁷ The stringency of these requirements will vary from case to case in accordance with the kind of data processing involved. Thus, exactly which types of data processing will meet the requirements is a question of fact that cannot be answered conclusively at present. It is clear, though, that the requirements will be met if a MD registers only those data as are necessary for enforcing the terms of a contract entered into with a purchaser. Such data would probably include the purchaser’s name and address, the name and price of the purchased product, together with the date of purchase.

With respect to registration and further processing of browser-related data, the condition in para (b) will not serve to justify this when the data subject is purely browsing. The condition will only be relevant once the data subject actively asks the MD to prepare for an imminent purchase transaction.

The condition set down in para (c) could be relevant insofar as the controller (eg, the MD) has legal obligations towards other ECMS actors (eg, the CP and creator). At the same time, though, it could be argued that the term “legal obligation” in para (c) is to be construed narrowly, such that it does not cover purely contractual obligations. This argument is based on the fact that para (c) otherwise could be used by data controllers to create at will a legal competence to process personal data simply by writing up a contract (to which the data subject is not party). The argument would also seem to be supported by the existence and wording of para (b).⁴⁸

If an appropriate legal obligation is found to exist between ECMS actors, a question of fact will again arise as to what data are necessary to process in order to comply with the obligation. The necessity criterion here will be the same as in relation to paras (b), (d), (e) and (f). It is doubtful that the criterion will be met in the case of registration and further processing of data relating to persons who only browse. Hence, the use of cookies mechanisms to register such data will fall outside the scope of para (c).

⁴⁷ Cf Art 6(1)(c) of the Directive (personal data must be “not excessive” in relation to the purposes for which they are processed). Note too that the European Court of Human Rights has interpreted the term “necessary” in Art 8(2) of the ECHR along similar lines: see further section 3 below.

⁴⁸ Note that Art 7(c) in an earlier proposal for the Directive referred to an “obligation imposed by national law or by Community law”. See European Commission 1992: 17 & 72.

The condition laid out in para (f) is the most flexible and open-ended of the ECMS-relevant conditions in Art 7. The Directive provides little useful guidance on how the various interests in para (f) are to be balanced. Who, for example, is intended to undertake the interest balancing? Recital 30 states that, in balancing the various interests, Member States are to guarantee “effective competition”; Member States may also determine conditions for use of personal data “in the context of the legitimate ordinary business activities of companies and other bodies”, and for disclosure of data to third parties for marketing purposes. Otherwise, the Directive leaves it up to the Member States to determine how the interests are to be balanced.

An interesting issue in relation to para (f) is the extent to which it may justify the use of cookies mechanisms that involve non-consensual registration of the fact that a person has accessed a MD’s server. The issue is, of course, only pertinent insofar as the data registered (eg, the address of the visitor’s machine) can properly be viewed as “personal” pursuant to Art 2(a) of the Directive. While such cookies mechanisms may serve the legitimate interests of, say, MDs, it is difficult to see how they can be seen as “necessary” for satisfying these interests, though the propriety of such an assessment all depends on how the interests are defined and on exactly what data are registered. If the interests are defined in terms of achieving “best possible conditions for product marketing”, the use of cookies mechanisms might be seen as necessary, even if those mechanisms only generate relatively coarse-grained data about consumer preferences. But even if such mechanisms are found necessary, they may well be “trumped” by the data subjects’ interests in privacy, integrity and autonomy. The strength of these interests will increase in tact with the increase in detail and sensitivity of the data generated by the cookies mechanisms (see further the discussion in section 2.3.2 below).

To sum up, the four conditions discussed above should, in combination, enable the registration and further processing of certain types of purchaser-related data by ECMS actors. They may also allow for the registration and further processing of certain types of browser-related data, though to a much lesser extent than in the case of data on purchasers.

2.3.2 Especially Sensitive Data

The conditions for lawful registration and further processing of personal data are sharpened by Art 8 of the DPD in relation to certain kinds of especially sensitive data. Most other data protection laws (but not all)⁴⁹ also contain extra safeguards for designated categories of especially sensitive data, but there is considerable variation in the way in which these data categories are described. The DPD lists the following data categories as deserving extra protection: data on a person’s “racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and ... health or sex life” (Art 8(1)). Data on “offences, criminal convictions or security measures” are also afforded extra protection under Art 8(5), though these are scarcely relevant in the context of ECMS operations.

⁴⁹ See, eg, the data protection laws of the Pacific-rim countries.

There is some uncertainty whether the list of data categories in Art 8(1) is exhaustive or not. We will not go into this issue in detail. It suffices to say that there is nothing on the face of the Directive to indicate that the list is not exhaustive, though the loose way in which the categories are formulated makes it possible to interpret them broadly.

An ECMS might involve the processing of some of the above types of data inasmuch as certain personal preferences of purchasers and/or browsers are registered by a MD. If, for instance, a purchaser enters into a contractual transaction for the use of an information product that concerns a particular religious or sexual theme, and the product is registered against the purchaser's name (or pseudonym or other unique identifier), it could be argued that sensitive data about the purchaser have thereby been processed. But it could also be contended that the connection between the product's theme and the purchaser's personality in such a case is too remote: ie, just because a person buys usage rights with respect to a particular product does not necessarily mean that the product reflects the person's own taste; he/she may simply be sampling or analysing a range of products. The strength of this contention will depend on several factors, including the nature of the product (eg, an academic treatise on satanism will tend to say less about the purchaser's personal religious inclinations than, say, a video-clip depicting satanic rituals for the purpose of viewer enthrallment) and the nature of the transaction (eg, a one-off transaction will also tend to say less about the purchaser's personal preferences than a series of transactions involving information products that focus on a similar theme). The same sort of analysis will apply with respect to registration of products in which a particular browser shows interest.

Article 8 of the Directive opens with a prohibition on the processing of the above categories of data, but follows up with a list (in Art 8(2)) of alternative exemptions to this prohibition. In the context of ECMS operations, the relevant exemptions are found in Art 8(2)(a) – ie, processing may occur if the data subject explicitly consents to it (except where national laws override this condition) – and Art 8(2)(e) – ie, processing may occur if the data in question “are manifestly made public” by the data subject, or their processing is “necessary for the establishment, exercise or defence of legal claims.

With regard to the first-mentioned exemption, it should be noted that consent must be “explicit” (cf the more lenient criterion of non-ambiguity in Art 7(a)). This means that the process of requesting and providing consent must occur as a formally separate process to the actual purchase transaction. There must be a specific request by the MD for permission from the purchaser/browser to process the data in question, followed by a specific reply in the affirmative. Arguably too, there must be some sort of record made of the request and reply, with measures in place to keep the record secure from unauthorised access and modification. It is worth noting § 3(7) of the German *Teleservices Data Protection Act* which allows for electronic declaration of consent if the teleservice provider ensures that

1. such consent can be given only through an unambiguous and deliberate act by the user,
2. consent cannot be modified without detection,
3. the creator can be identified,
4. the consent is recorded and

5. the text of the consent can be obtained by the user on request at any time.

These conditions apply even in relation to non-sensitive data.

As for the second-mentioned exemption in Art 8(2)(e), one issue concerns the meaning of “manifestly made public”. Given the nature of the data involved, the phrase should arguably be interpreted fairly narrowly as indicating an *obvious and conscious readiness* by the data subject to make the data available to *any* member of the general public. The extent to which this condition will be satisfied in the context of an ECMS will depend on the data subject’s understanding of the operational parameters of the particular ECMS. If the data subject believes that the ECMS operates as a closed system *vis-à-vis* other systems (ie, that ECMS actors observe strict rules of confidentiality when handling purchaser-/browser-related data), it is difficult to see the condition being satisfied.⁵⁰

Another issue in relation to Art 8(2)(e) concerns the meaning of “legal claims”. Again, it is arguable that the phrase is not intended to cover claims arising from purely contractual obligations, for the same reasons as are given with respect to Art 7(c) (see section 2.3.1 above). Indeed, the sensitive nature of the data involved is an extra ground for reading the phrase in this way. Nevertheless, it is quite possible that national legislation implementing the Directive will allow for data processing in order for a data controller to defend a legal claim in the form of copyright, as the latter is statutorily anchored. Note, though, that the latter claim will attach primarily to the copyright holder and not, say, the MD. Another issue, though, will be the extent to which such processing is “necessary” (as defined in relation to Art 7) for the defence of such a legal claim. Here, the necessity criterion should be interpreted strictly since the data in question are regarded as especially sensitive. Thus, “necessary” should be held as denoting a stringent standard of indispensability. For instance, while initial registration of such data might be found indispensable for ensuring that copyright is not breached, it will be incumbent on the MD (or whoever is data controller) to delete or anonymise the data once the relevant interests of the copyright holder can be safeguarded in some other way.

Finally, it is worth noting that although the USA has not yet enacted data protection legislation regulating the private sector as comprehensively as the equivalent legislation does in West European countries, it has singled out for special regulation several sectors of what we might call the informational distribution industry. We refer here especially to the Video Privacy Protection Act of 1988,⁵¹ the Cable Communications Privacy Act of 1984,⁵² together with state legislation regulating the processing of library records.⁵³ All of these pieces of legislation aim at restricting the registration and further processing of data on information consumers’ viewing/reading/listening habits. For our purposes, these laws

⁵⁰ It is even difficult to see the condition being satisfied in relation to non-virtual shopping: while the purchase of, say, a book in a non-virtual shop will typically be a public act in the sense that any member of the public can incidentally witness the transaction, the purchaser will rarely intend a record of that transaction to be made available (in non-anonymous format) to any member of the public.

⁵¹ Codified at § 2710 of Title 18 of the United States Code (USC).

⁵² Codified at § 551 of Title 47 of the USC.

⁵³ See, eg, § 4509 of the New York State Civil Practice Law and Rules. See further the references given in Cohen 1996: n 214.

serve to underline the fact that such data are generally regarded as deserving of special protection.

2.4 Anonymity

Article 6(1)(e) of the DPD provides for the anonymisation of personal data once the need for person-identification lapses: ie, personal data must be “kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed”. The same rule is contained in many other data protection laws too. The rule should be seen in conjunction with the stipulation in Art 6(1)(c) – also found in numerous other data protection laws – that personal data be “not excessive” in relation to the purposes for which they are processed.⁵⁴ Read together, these rules arguably embody a general principle requiring, as a point of departure, transactional anonymity unless there are overriding legitimate interests to the contrary. Such a principle should also be read as requiring that active consideration be given to crafting technical solutions for ensuring transactional anonymity.

It is worth noting that the issue of transactional anonymity is expressly addressed in the German *Teleservices Data Protection Act*. The Act provides, *inter alia*, that “[t]he design and selection of technical devices to be used for teleservices shall be oriented to the goal of collecting, processing and using either no personal data at all or as few data as possible” (§ 3(4)). Further, the Act stipulates that a teleservice provider “shall offer the user anonymous use and payment of teleservices or use and payment under a pseudonym to the extent technically feasible and reasonable” and that the user “shall be informed about these options” (§ 4(1)).⁵⁵

The issue of transactional anonymity is also specifically addressed in some policy documents issued recently. The *Budapest-Berlin Memorandum on Data Protection and Privacy on the Internet*, adopted 19.11.1996 by the International Working Group on Data Protection and Telecommunications, states, *inter alia*, that, “[i]n general, users should have the opportunity to access the Internet without having to reveal their identity where personal data are not needed to provide a certain service”.⁵⁶ Recommendation 3/97, adopted 3.12.1997 by the Working Party on the Protection of Individuals with regard to the Processing of Personal Data (hereinafter termed “Data Protection Working Party”) set up pursuant to Art 29 of the DPD, follows the thrust of the above Memorandum by urging the European Commission to develop proposals for securing transactional anonymity on the Internet.⁵⁷ In the USA, the Information Infrastructure Task Force adopted on 6.6.1995 a set of Principles for Providing and Using Personal Information which stipulate, *inter alia*, that “[i]ndividuals should be able to safeguard their own privacy by having ... [t]he opportunity to remain anonymous when appropriate”

⁵⁴ Note too the necessity criterion in Arts 7 and 8, discussed in the preceding sections.

⁵⁵ Note also § 4(4), set out in section 2.5.2 below.

⁵⁶ See further International Working Group on Data Protection and Telecommunications 1996.

⁵⁷ See Data Protection Working Party 1997b.

(Principle III.B.4).⁵⁸ The Australian Privacy Charter, adopted in December 1994, contains a principle of “anonymous transactions” which states: “People should have the option of not identifying themselves when entering transactions”.⁵⁹ None of these policy instruments, however, have the force of law. Nevertheless, they demonstrate an increasing concern in many countries to create conditions conducive to anonymity in cyberspace.

In light of the above, it is advisable that those engaged in the design and establishment of an ECMS “build in” possibilities for anonymising transactions wherever technically feasible and wherever the interest in purchaser/browser anonymity is not overridden by other legitimate interests.⁶⁰ There would appear to be, for instance, no overriding interests to justify the flow of transactional data from a MD to an MSP in other than anonymised (eg, aggregate) form.

2.5 Purpose Specification and Finality

2.5.1 Generally

As noted in the Introduction, a central principle in most data protection laws is that of purpose specification (sometimes also termed the finality principle). The principle is expressed in Art 6(1)(b) of the DPD as follows:

[Member States shall provide that personal data must be] collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that the Member States provide appropriate safeguards.

In an ECMS context, this sort of rule has obvious repercussions for the secondary uses to which MDs, CPs and other ECMS actors will be able to put purchaser-/browser-related data.

We can see the principle in Art 6(1)(b) as grounded partly in concern for ensuring that data are processed in ways that conform with data subjects’ reasonable expectations.⁶¹ We can also see the principle as grounded in concern for ensuring that data are used for purposes to which they are suited (ie, a concern for adequate information quality).

From the wording of Art 6(1)(b), it is apparent that the purposes for which, say, a MD registers data on a purchaser or browser must be defined, documented and announced in

⁵⁸ See Information Infrastructure Task Force 1995.

⁵⁹ The Charter is the private initiative of a group of concerned citizens and interest groups; it has not been conferred any official status by a government body.

⁶⁰ See further section 4 below. See also the “Consensus Conclusions” of the First IMPRIMATUR Consensus Forum set out in section 1.3 above.

⁶¹ In this regard, note the Fairness Principle adopted by the US Information Infrastructure Task Force (“[i]nformation users should not use personal information in ways that are incompatible with the individual’s understanding of how it will be used, unless there is a compelling public interest for such use”): see Information Infrastructure Task Force 1995.

advance of registration. They must also be notified to the data subject.⁶² Further, they must be “legitimate”. Arguably, the term “legitimate” denotes a criterion of social acceptability which is broader than that of lawfulness, though it is difficult to determine how much it is broader. The conditions laid down in Arts 7 and 8 (see section 2.3 above) provide some, but not exhaustive, guidance on the ambit of the legitimacy criterion. At the same time, it is apparent that a data controller cannot define the purposes of data processing in the same broad and diffuse terms as are found in Arts 7 and 8: use of the adjective “specified” in Art 6(1)(b) indicates that the purposes need to be delineated more concretely and narrowly.

The phrase “not incompatible” could be read as meaning simply “compatible”, though use of the double negative perhaps denotes a slightly less stringent standard than that of straight compatibility. However, if we accept that one of the underlying concerns of the purpose specification principle is to ensure that data are processed in conformity with data subjects’ reasonable expectations, then any secondary purpose should not pass the test of compatibility/non-incompatibility unless the data subject is able, objectively speaking, to read that purpose into the purpose(s) first specified, or the secondary purpose is otherwise within the ambit of the data subject’s reasonable expectations. It is doubtful, for example, that the purpose of marketing would satisfy this test if the primary purpose for the data processing were specified only in terms of billing.

The rule in Art 6(1)(b) is supplemented by Arts 6(1)(c) and 6(1)(d). The latter provision requires that data be “accurate and, where necessary, kept up to date”, while Art 6(1)(c) stipulates that personal data must be “adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed”. The criteria in sub-para (c) – particularly that of non-excessiveness – reinforce the necessity criterion in Arts 7 and 8. If, say, a MD announces that he/she/it registers purchaser-related data for the purpose of billing the data subjects, the rule in Art 6(1)(c) will not allow the MD to register more purchaser-related data than is necessary for billing purposes – unless the data subject consents otherwise.

The provisions of both the EU ISDN Directive and Germany’s *Teleservices Data Protection Act* signal an intention on the part of European legislators to enforce a fairly stringent version of the purpose specification principle in the relations between telecommunications service providers and service users/subscribers. Both laws severely restrict the purposes for which telecommunications service providers may store and utilise data on users/subscribers without the latter’s consent. For instance, the ISDN Directive’s basic point of departure is that traffic data on users/subscribers which are processed to establish “calls” must be erased or made anonymous upon termination of the call (Art 6(1)).⁶³ Article 6(2) of the Directive permits service providers to process only such data on users/subscribers as are necessary for billing purposes and interconnection

⁶² See also Arts 10 and 11 of the Directive set out below in section 2.6.

⁶³ From the use of the word “call”, it appears that this provision is intended to regulate ordinary telephone calls only, but this would seem inconsistent with the broad definition of “telecommunications service” in Art 2(d) of the ISDN Directive which refers to “services whose provision consists wholly or partly in the transmission and routing of signals on telecommunications networks, with the exception of radio- and television broadcasting”.

payments. This processing is “permissible only up to the end of the period during which the bill may lawfully be challenged or payment may be pursued” (Art 6(2)). The data may only be used for the purpose of marketing the provider’s own services if the subscriber has consented (Art 6(3)). Similar rules are found in §§ 5 and 6 of Germany’s *Teleservices Data Protection Act*.

2.5.2 Marketing

Some data protection laws (particularly those enacted recently) show an express concern to limit the extent to which data controllers can exploit personal data for the purpose of marketing goods and services *vis-à-vis* the data subjects. Two main sets of measures tend to be pursued. One set of measures is to give data subjects a right to object to direct marketing; the other set of measures is to restrict data controllers’ ability to build up personality profiles of data subjects.

An important instance of the first-mentioned set of measures is Art 14(b) of the DPD. According to Art 14(b), EU Member States are to provide a data subject with two options: (i) “to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing”; or (ii) “to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses”. Member States are required to take “necessary measures to ensure that data subjects are aware of” the right to object pursuant to Art 14(b).

Another important instance of this sort of right to object is § 5(2) of Germany’s *Teleservices Data Protection Act* which provides that “[p]rocessing and use of contractual data for the purpose of advising, advertising, market research or for the demand-oriented design of the teleservices are only permissible if the user has given his *explicit consent*” (emphasis added).

Of more global relevance are the *Revised Guidelines on Advertising and Marketing on the Internet* adopted 2.4.1998 by the International Chamber of Commerce (ICC). These Guidelines (hereinafter termed “ICC Guidelines”) contain provisions restricting unsolicited commercial messages over the Internet. Article 5(6) of the Guidelines states:

Advertisers and marketers should not send unsolicited commercial messages online to users who have indicated that they do not wish to receive such messages. Advertisers and marketers should make an online mechanism available to users by which the users can make known to the advertisers that they do not wish to receive future online solicitations⁶⁴

In North America, the *Individual Reference Services Industry Principles* adopted 10.6.1997 by CDB Infotek *et al* contain a principle dealing expressly with use of information on minors: “[w]here an individual is identified in the product or service as

⁶⁴ ICC 1998.

being under the age of 18, no Non-Public Information about that individual should be provided for non-selective commercial distribution without parental consent”.⁶⁵

Regarding the second set of measures (ie, those concerned to restrict profiling), Germany’s *Teleservices Data Protection Act* appears to provide the most restrictive regulations. The Act stipulates that teleservice providers are to take measures to ensure that “personal data relating to the use of several teleservices by one user are processed separately; a combination of such data is not permitted unless it is necessary for accounting purposes” (§ 4(2)(4)). Moreover, the creation of user profiles is allowed only if pseudonyms are employed, and the “[p]rofiles retrievable under pseudonyms shall not be combined with data relating to the bearer of the pseudonym” (§4(4)).

Also of relevance for profiling is Art 15(1) of the DPD. This provision grants a person the right “not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc”. The right is not absolute; a person may be subjected to such decisions if they are, in summary, taken pursuant to a contract with the data subject or authorised by law, *and* provision is made for “suitable measures” to safeguard the person’s “legitimate interests” (Art 15(2)). Note that the right does not restrict the creation of profiles by fully automated means; rather, it restricts certain *uses* of such profiles.

The above sorts of provisions dealing with profiling are not yet commonplace in data protection laws, though this is likely to change in the near future.

All of the provisions canvassed in this section will set limits on the purposes for which ECMS actors will be able to employ purchaser-/browser-related data. While there will exist some legal opportunities for using these data for purposes beyond what the data subjects might reasonably expect, it would be advisable that ECMS actors show reticence in exploiting such opportunities, not least in order to build up consumer trust and confidence in ECMS operations.

2.6 Orientation of Data Subjects

The EU Data Protection Directive sets down several sets of rules aimed at orienting persons about the processing of data on them. One set of rules grant persons the right to gain access to data kept on them by other persons and organisations. The most important formulation of this right is given in Art 12 as follows:

Member States shall guarantee every data subject the right to obtain from the controller: (a) without constraint at reasonable intervals and without excessive delay or expense:

⁶⁵ CDB Infotek *et al* 1997. By “Non-Public Information” is meant “[i]nformation about an individual that is of a private nature and neither generally available to the public nor obtained from a public record”.

- confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,
- communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,
- knowledge of the logic involved in any automated processing of data concerning him at least in the case of the automated decisions referred to in Article 15(1).

Broadly similar sets of access rights are a central feature of all data protection laws.

A second set of rules provides that data controllers must, of their own accord, inform data subjects about their data-processing practices. Article 10 of the Directive stipulates that when data are collected from the data subject, he/she must be informed of “at least” the identity of the data controller and the latter’s representatives, together with the intended purposes of the data processing (unless the data subject already has this information); other types of information may also be provided insofar as is “necessary” in the circumstances “to guarantee fair processing in respect of the data subject”. With a few exceptions, Art 11 contains similar requirements in cases when data are not collected directly from the data subject.

Such rules are not yet commonplace in data protection legislation but will become so under the the influence of the Directive.

Germany’s *Teleservices Data Protection Act* contains several provisions that elaborate upon and extend the rules in Arts 10 and 11 of the DPD. The first of these provisions states that a user of teleservices “shall be informed about the type, scope, place and purposes of collection, processing and use of his personal data” (§ 3(5)). The provision goes on to address the use of cookies mechanisms, stipulating that, “[i]n case of automatic processing, which permits subsequent identification of the user and which prepares the collection, processing or use of personal data, the user shall be informed prior to the beginning of the procedure”. Another provision of note requires that the user be informed about his/her right to withdraw his/her consent to a given data-processing operation (§ 3(6)). Finally, § 4(1) requires the user to be notified of whatever options exist for making anonymous or pseudonymous use and payment of teleservices.

Also noteworthy is the following Notice Principle included in the data protection principles adopted by the US Information Infrastructure Task Force. This principle provides that

[i]nformation users who collect personal information directly from the individual should provide adequate, relevant information about: 1) Why they are collecting the information; 2) What the information is expected to be used for; 3) What steps will be taken to protect its confidentiality, integrity, and quality; 4) The consequences of providing or withholding information; and 5) Any rights of redress.⁶⁶

⁶⁶ Information Infrastructure Task Force 1995. Cf the more generally worded guideline in the Budapest-Berlin Memorandum (“[s]ervice providers should inform each potential user of the Net unequivocally about the risk to his privacy”): see International Working Group on Data Protection in Telecommunications 1996.

The ICC Guidelines provide that “[a]dvertisers and marketers of goods and services who post commercial messages via the Internet should always disclose their own identity and that of the relevant subsidiary, if applicable, in such a way that the user can contact the advertiser or marketer without difficulty” (Art 2). Further, “[a]dvertisers and marketers should disclose the purpose(s) for collecting and using personal data to users” (Art 5(1)).

2.7 Security Measures

Data protection laws typically contain provisions requiring data controllers to take steps to ensure that personal data are not destroyed accidentally and not subject to unauthorised access, alteration, destruction and disclosure. A representative provision to this effect is Art 17(1) of the DPD which stipulates:

[Data controllers] must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

A controller must also ensure – by way of contract or other legal act (Art 17(3)) – that data processors engaged by him/her/it provide "sufficient guarantees in respect of the technical security measures and organizational security measures governing the processing to be carried out" (Art 17(2)). The latter requirements are supplemented in Art 16 which provides that “[a]ny person acting under the authority of the controller or ... processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law".

Similar provisions are set out in Arts 4 and 5 of the EU ISDN Directive. Article 5 is especially relevant for ECMS operations. Amongst other things, it prohibits “listening, tapping, storage or other kinds of interception or surveillance of communications, by others than users, without the consent of the users concerned, except when legally authorised, in accordance with Article 14(1)” (Art 5(1)). This provision is sufficiently broad to impinge upon the ability of ECMS actors to monitor the activities of purchasers and browsers. We can see the provision as grounded partly in a concern to uphold the right to privacy of communications – a right embodied in, *inter alia*, Art 8(1) of the ECHR.⁶⁷

At the same time, Article 14(1) permits derogation from Art 5(1) insofar as is “necessary ... to safeguard ... prevention, investigation, detection and prosecution of criminal offences ...”. Moreover, Art 5(2) states that the prohibition in Art 5(1) “shall not affect any legally authorised recording of communications in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication”. Both derogations appear to derive from the criteria listed

⁶⁷ See further section 3.

in Art 8(2) of the ECHR. Both may be relied upon to justify some monitoring of purchaser activities in an ECMS context, though probably not the activities of browsers.

2.8 Transborder Data Flows

In the context of an ECMS, four situations could arise involving the flow of personal data on purchasers or browsers across national borders:

1. the purchaser/browser is situated in one EU Member State with the MD (or other ECMS actor) situated in another EU Member State;
2. the purchaser/browser is situated in an EU Member State and the MD (or other ECMS actor) is situated in a state outside the EU (ie, a so-called “third country”);
3. the MD (or other ECMS actor) is situated in an EU Member State, while another ECMS actor is situated in a third country;
4. the purchaser/browser is situated in a third country, while the MD (or other ECMS actor) is situated in an EU Member State.

With regard to situation 1, the DPD stipulates in Art 1(2) that the flow of personal data between EU Member States cannot be restricted for reasons concerned with protection of the “fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data”.

As for transfer of personal data to countries outside the EU (situation 2), this is regulated in Arts 25 and 26 of the Directive. The basic rule is that transfer “may take place only if ... the third country in question ensures an adequate level of protection” (Art 25(1)). No definition or indication of the meaning of “adequate” is provided by the Directive, but it probably denotes a less stringent standard than that of equivalence.⁶⁸ Article 25(2) states that the “adequacy” criterion cannot be fleshed out in the abstract; rather, “adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations”. From this provision, it is clear that account is to be taken not just of the content and application of third countries’ legislation that deals specifically with data protection; other rules and practices may also be relevant.⁶⁹

According to the Data Protection Working Party, the issue of adequacy essentially involves assessing the “degree of risk to the data subject that the transfer involves”.⁷⁰ Interestingly (from an ECMS perspective), the Working Party includes in its list of data transfers that “pose particular risks to privacy” the following: “repetitive transfers involving massive volumes of data (such as transactional data processed over telecommunications networks, the Internet etc)” and “transfers involving the collection of data in a particularly covert or clandestine manner (eg, Internet cookies)”.⁷¹

⁶⁸ See also Schwartz 1995: 473 & 487; Ellger 1991: 131. 131.

⁶⁹ See also Terwangne & Louveaux 1997: 244.

⁷⁰ Data Protection Working Party 1997a.

⁷¹ *Ibid.*

It is not entirely clear from the Directive if adequacy may be assessed on a sectoral as opposed to national basis; ie, if the whole of the third country's legal regime on data protection is to be assessed or just those parts of the regime which deal specifically with the data concerned. The focus of Art 25(2) on particular "data transfer operations" suggests that sector-specific as opposed to national assessment is possible.⁷²

Some uncertainty reigns also over whether the standards in the Directive constitute the only point of reference for determining adequacy. Article 25(1) and recital 60 suggest that the legislative standards adopted by an EU Member State pursuant to the Directive – standards which may be more stringent in certain respects than those set by the Directive – may constitute the primary point of departure for assessing the adequacy of data protection afforded by a third country.⁷³

Derogations from the rule in Art 25(1) are set out in Art 26. Of particular relevance for ECMS operations, are the following derogations:

- (a) the data subject has given his consent unambiguously to the proposed transfer; or
- (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or
- (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or
- (d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims

These conditions for transfer are broadly similar to some of the conditions for data processing laid down in Art 7, such that interpretation of the latter will be of relevance for interpretation of the former. Regarding the condition in Art 26(1)(a) – dealing with consent – the MD (or other ECMS actor) must take active measures to make the purchaser/browser aware of the fact that data will be transferred to a third country (ie, consent must be given "to the proposed transfer", not processing generally). The data subject must also be informed of the identity of the country of destination, together with the fact that the latter does not provide adequate protection.⁷⁴

As for the condition laid down in para (b) above, this should be met fairly easily in the context of situation 2. Otherwise we refer to what is written in relation to Art 7(b) in section 2.3.1 above. It has been claimed that the condition in Art 26(b) will only be satisfied if the data subject is also "made aware that once the data has [*sic*] been transferred to the third country for the contract in question, there are no means of ensuring that the data will not be further used for other purposes ...".⁷⁵ From a data protection perspective, the latter requirement is sensible *de lege ferenda* but is by no means obvious from the wording of para (b). Such a requirement, however, could be

⁷² See also Data Protection Working Party 1997a; Greenleaf 1995: 106.

⁷³ See also Schwartz 1995: 487. Article 25(1) states that "transfer may take place only if, *without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive*, the third country ... ensures an adequate level of protection" (emphasis added). According to recital 60, "transfers to third countries may be effected only in full compliance with the provisions adopted by the Member States pursuant to this Directive".

⁷⁴ See also Terwangne & Louveaux 1997: 244.

⁷⁵ *Ibid*, 245.

implied from the more general fairness criterion that is expressly embodied in Art 6(1)(a) of the Directive and particularised in the principles of purpose specification in Art 6(1)(b) and individual participation in Arts 10–12. There can be little doubt that this fairness criterion also permeates Arts 25 and 26.

The condition in para (d) should be met fairly easily, inasmuch as the transfer serves to safeguard copyright. Purely contractual obligations will probably fall outside the scope of the phrase “legal claims”, for the same reasons as are given in relation to Arts 7(c) and 8(2)(e) in section 2.3 above.

Another provision of note is Art 26(2), which permits transfer in derogation of Art 25(1)

where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.

It is arguable that “appropriate contractual clauses” in this provision must be enforceable by data subjects. Thus, where doctrines on privity of contract apply, contracts to which data controllers/processors/recipients are the sole parties will probably be insufficient to result in “adequate safeguards” for the purposes of Art 26(2).

All in all, it is difficult to see that a transfer of personal data in the context of situation 2 will not meet one or more of the above derogations. In other words, the issue of what constitutes adequate protection pursuant to Art 25 is likely to be of marginal significance here.

Regarding situation 3, it should first be noted that Arts 25 and 26 will only apply insofar as the data transferred are “personal” pursuant to Art 2(a). Thus, if the data flowing from a MD to an MSP are anonymised (which we argue should probably be the case: see section 2.4 above), the Directive will not impinge on the flow whatsoever. If the data are not anonymised, and the data are intended to be transferred to a country that does not provide adequate protection pursuant to Art 25(2), the transfer could arguably be justified under Art 26(1)(c) or (d), or Art 26(2). A sticking point in relation to Art 26(1)(c) will be whether or not the transfer could properly be said to be in the interest of the data subject (ie, the purchaser or browser).

As for situation 4, transfers of purchaser-/browser-related data will not be affected by the Directive because the flow of data will be *into* the EU – a situation not addressed by Arts 25 or 26. However, if these data are subsequently passed on to an ECMS actor in a third country (ie, situation 3), the Directive will apply.

2.9 General Derogations

The Directive gives EU Member States the opportunity of adopting legislative measures that derogate from the provisions in Arts 6(1), 10, 11, 12 and 21, if it is necessary to safeguard, *inter alia*, “the prevention, investigation, detection and prosecution of criminal

offences ...” (Art 13(1)(d)), or “the protection of the ... rights and freedom of others” (Art 13(1)(f)).

Both exemptions are of relevance in an ECMS context, and could be used by copyright holders or their representative organisations as leverage points for pressuring EU Member States into drafting data protection laws that are more “ECMS-friendly” than Arts 6(1), 10, 11(1), 12 and 21 would *prima facie* allow.

Another such leverage point could be Art 9 which requires Member States to derogate from all of the Directive’s provisions canvassed so far in this report, with regard to “processing of personal data carried out solely for ... the purpose of artistic or literary expression” but only if the derogations are “necessary to reconcile the right to privacy with the rules governing freedom of expression”. Of course, Art 9 will only be relevant for ECMS operations insofar as the basic rationale of the latter can properly be characterised as the promotion of freedom of artistic or literary expression – a debatable point!

3. Application of Art 8 of the ECHR to ECMS Operations

As noted in the Introduction, there is a paucity of Art 8 case law dealing specifically with the data-processing activities of private sector bodies. Nevertheless, on the basis of the case law dealing with the practices of public authorities, it could be plausibly argued that the processing of purchaser-/browser-related data in an ECMS context will interfere with the data subject's right to respect for private life under Art 8(1) if the following cumulative conditions are met:

- (i) the data reveal details about the data subject's personality (eg, his/her preferences);
- (ii) the data are processed without the data subject's knowledge or consent; and
- (iii) the processing potentially casts the data subject in a negative light or could result in a restriction of the data subject's freedom of choice.⁷⁶

An interference will also arise if a person's communications are monitored by others without his/her consent and the monitoring is not what the person could reasonably expect.⁷⁷

Denial of access to information about oneself which is kept by others will ordinarily not amount to an interference with Art 8(1). Nevertheless, Art 8(1) does embody an interest for persons to be given access to information that is essential for their psychological well-being and understanding of personal identity.⁷⁸ Further, the protection of this interest can arise as a positive obligation on the part of State Parties to ensure respect for a person's right under Art 8(1).⁷⁹ However, it is doubtful that purchasers or browsers would be given, pursuant to Art 8, a right of access to information gathered about them by ECMS actors, as access to such information can probably not be regarded as essential for their personal development in the manner outlined above.

Article 8(2) sets down a number of conditions for justifying an interference with an Art 8(1) right. Firstly, there must be some sort of legal authority (not necessarily statutory in character) for the interference. Secondly, the legal measure concerned must be accessible to the data subject and sufficiently precise to allow him/her reasonably to foresee its consequences.⁸⁰ Thirdly, the interference must have been carried out in order to achieve one or more of the aims listed in Art 8(2). The fourth and final justificative criterion is that the interference must be "necessary in a democratic society"; ie, it must "correspond to a pressing social need" and be "proportionate to the legitimate aim pursued".⁸¹ In applying these criteria, the European Court of Human Rights accords State Parties a "margin of appreciation", allowing the judgement of what is appropriate in the circumstances of the particular case to be determined to some extent by the national

⁷⁶ See further Bygrave 1998b.

⁷⁷ *Halford v United Kingdom* (1997) Reports of Judgements and Decisions 1997-III, 1004, paras 44–46.

⁷⁸ *Gaskin v United Kingdom* (1989) A 160, para 49.

⁷⁹ *Id.*

⁸⁰ See, eg, *Sunday Times v United Kingdom* (1979) A 30, para 49.

⁸¹ See, eg, *Leander v Sweden* (1987) A 116, para 58.

authorities.⁸² It is important to note, however, that the conditions in Art 8(2) are only directly relevant with respect to interferences incurred by the actions of *public* authorities. It seems likely that ECMS operations will ordinarily be executed by private sector bodies only, though some ECMS actors might conceivably operate in a semi-public capacity.

If ECMS operations involve private sector bodies only, the main issue under Art 8 will concern the nature and extent of a State Party's positive obligations to ensure that these bodies respect the Art 8(1) right of purchasers/browsers. In assessing the character of such obligations, the Court will attempt to strike a "fair balance" between the "general interests of the community and the needs of the individual".⁸³ In this process, the Court will have some regard to the aims specified in Art 8(2).⁸⁴ At the same time, it should be kept in mind that the Court is likely to give State Parties a broad margin of appreciation when assessing the obligations of public authorities in this context, because the data processing concerned will be carried out by a private actor. Motivating the Court's policy in this regard will be a desire not to prompt State intervention in the private sphere which could in turn curtail the very interests that Art 8 or other ECHR provisions (particularly Art 10) are intended to safeguard.⁸⁵ Nevertheless, it is very doubtful that the Court will refrain from obliging a State Party to enact legal rules embodying core data protection principles and to apply these rules to private bodies. This assumes, of course, that these rules contain much the same exemption clauses as are found, say, in the DPD.

⁸² The extent of this margin of appreciation varies from case to case and depends on the Court's appraisal of a variety of factors. These include the importance of the right that is breached, the importance of the "legitimate aim" for which the breach is committed, and the conformity of the breach to a relevant pan-European practice. For detailed discussion of these factors, see, eg, Harris *et al* 1995: 290–301, 344–353.

⁸³ See, eg, *Gaskin v United Kingdom* (1989) A 160, para 42.

⁸⁴ *Id.* One such aim is the "prevention of crime"; another is the "protection of the rights and freedoms of others". Both aims are relevant for ECMS operations.

⁸⁵ See further Clapham 1993: 220ff.

4. Privacy-Enhancing Technologies

Privacy-enhancing technologies (PETs) are technical and organisational tools for reducing or eliminating the collection and further processing of data that can be used to identify an individual person.⁸⁶ Most focus has hitherto been placed on PETs that rely on the application of public-key/asymmetric methods of encryption. On the basis of these methods, it is possible to create mechanisms for allowing a person, such as a purchaser in an ECMS, to operate relatively anonymously in his/her direct contact with another person/organisation, such as a MD. There are two main mechanisms of interest here: digital cash and digital pseudonyms.

Currently, several forms of digital cash exist or are in the process of being tested.⁸⁷ Some are more privacy-enhancing than others but all are aimed at making it more or less difficult to link the purchase of a particular good or service to the purchaser. Digital pseudonyms, on the other hand, are aimed not so much at disconnecting the purchase of a particular good or service from the purchaser, but at making it difficult to find the real identity of the latter. At the same time, both types of mechanisms permit accountability and authentication with respect to the transaction entered into between the parties concerned.

There seems little or no valid technological or organisational reason for not incorporating these types of mechanisms into an ECMS such as the IMPRIMATUR Business Model. Indeed, as suggested in section 2.4 above, there is a legal (and ethical) need for such incorporation, derived partly from the principles of minimality and anonymity embodied in data protection laws. A system for identity escrow could be administered fairly easily by the Certification Authority (CA). In such a system, the CA would act as a trusted third party (TTP) for purchasers (and possibly browsers) as well as for the MD and other ECMS actors. As TTP, the CA would issue digital pseudonyms and hold the “master key” connecting these pseudonyms with the real identities of the pseudonym users.

In terms of data protection, it is important to note that PETs do not necessarily guarantee total transactional anonymity; as their name suggests, they merely augment the degree of privacy enjoyed by the data subjects.⁸⁸ Concomitantly, use of PETs will not necessarily result in the elimination of personal data as defined in, say, Art 2(a) of the DPD on data protection. A digital pseudonym is quite capable of being classified as “personal data” pursuant to most data protection laws, as the pseudonym may be indirectly linked to a specific person via the master key held by the TTP. However, a stringent interpretation of the “ease/probability-of-identification” criterion (see section 2.1) *might* result in pseudonymous data being regarded as non-personal (anonymous) if the TTP holding the master key operates with very strict measures to prevent the key being accessed by others.

⁸⁶ For general overviews of PETs, see Goldberg, Wagner & Brewer 1997, Burkert 1997a and 1997b.

⁸⁷ For a useful overview, see Froomkin 1996: Part III.

⁸⁸ Cf Cohen 1996: n 217 (“Anonymity objectives and privacy objectives overlap substantially. Nonetheless, the term “anonymity” describes a particularly stringent variety of “privacy”, and achieving true anonymity, as opposed to mere confidentiality, presents unique technological and procedural challenges”).

If the use of a PET is viewed as not eliminating the registration and other use of personal data, those ECMS operations in which the PET is applied will have to comply fully with the requirements of data protection laws; ie, the use of the PET will not take the ECMS operations outside the ambit of those legal requirements. However, the use of the PET will go a long way towards fulfilling the rules and recommendations set out in section 2.4 above. The use of the PET may also have legal relevance for processes whereby the interests of data controllers are to be weighed against the privacy interests of data subjects; ie, the PET may make it easier for the former interests to win out over the latter interests. Moreover, the use of a PET for a given data-processing operation may be relevant for assessing the extent to which that operation meets the criteria of “adequate protection” in Art 25(1) and “adequate safeguards” in Art 26(2) of the DPD (see section 2.8 above).

Finally, note should be taken of the possibility of configuring ECMS operations such that no personal data on purchasers or browsers are registered in the first place. For example, instead of registering such data as a means of enforcing copyright, each copyrighted information product could have microcode inserted into it which prevents purchasers or other users of the product from making more than one perfect copy of it. The privacy implications of such “blocking” mechanisms are discussed further below in section 5.4.2.

5. Copyright versus Privacy

5.1 Introductory Comments

Copyright and privacy may be considered as protecting similar interests. Obviously, the right to privacy may be viewed as a personality right. The same goes for the moral rights granted to the author under copyright law. Thus, it could be argued that copyright and the right to privacy are branches of the same tree.⁸⁹ The right to privacy can even be regarded as deriving from copyright: Warren and Brandeis, who could be called the “inventors” of the right to privacy, drew partly upon common law on copyright to support their thesis that English and US common law implicitly protected the individual’s right to privacy.⁹⁰

However, copyright and the right to privacy can collide if they work to the advantage of opposite parties. The intersection of the right to privacy and copyright law in this regard has not yet been thoroughly researched. The issue has become of particular interest only now that new technologies – as embodied, for example, in ECMS operations – enable the copyright-owner to monitor and control with relative ease the actual use that a person makes of a copyrighted work, thereby extending the reach of the copyright-holders. Until fairly recently, neither copyright, nor copyright-holders, invaded the private sphere of users of copyrighted materials. Copyright covered only acts that constituted a commercial exploitation of a work. Although user privacy tends not to be directly addressed in copyright law, the users’ right to privacy has arguably played a role in copyright in the analogue world.⁹¹ For instance, when copyright first entered into the users’ private sphere, both the copyright-holders’ interests and the user’s right to privacy were expressly taken into consideration. With regard to copyright in the digital environment, however, legislators seem to underestimate the users’ privacy and autonomy interests. Here the copyright-holders’ sphere of control manifestly overlaps the users’ private sphere. Through an ECMS, a copyright-holder *could* interfere with user privacy and autonomy to a greater extent than in the analogue environment.

In the rest of this report, we will attempt to describe these developments and investigate the possible impact of ECMS operations on user privacy. The purpose of this analysis is not to give an exhaustive or definitive description of the issue, but merely to provide for a rarely-taken line of approach which may provoke discussion.

5.2 Copyright vs. Privacy in the Analogue World

Until recently, the private “consumption” or use of copyrighted works fell outside the scope of copyright law. Copyright started off as a form of trade regulation. The first

⁸⁹ See Hughes 1988: 355. Hughes observes that the *droit de divulgation* could very well be viewed as a privacy right. See also Zimmerman 1992: 670–673, discussing *Salinger v Random House, Inc.*, 650 F Supp 413 (SDNY 1986), rev’d 811 F 2d 90 (2nd Cir), and cert denied, 484 US 890 (1987).

⁹⁰ Warren & Brandeis 1890: 204–213; see also Zimmerman 1992: 698–699.

⁹¹ See generally Haeger 1962.

copyright statute in England, the Statute of Anne of 1709, was intended to establish order in the publishing industry.⁹² Traditionally, the allocation of profits made from a copyrighted work has been one of the main purposes of copyright law.⁹³ This is expressed in the acts that are exclusively reserved for the copyright-holder, which are mainly acts associated with forms of commercial exploitation.⁹⁴ Private “analogue” use of copyrighted works, even the making of reproductions for private use, was generally not considered a commercial activity, and therefore not touched by copyright law.⁹⁵ Even though the consumers’ right to privacy tends not to be expressly considered in copyright law, copyright, with few exceptions, did not invade the private sphere of end-users.

In the following pages, we briefly describe the mechanisms incorporated in copyright law which have kept copyright outside the end-users’ private sphere. Thereafter follows an examination of the extent to which privacy considerations may have influenced copyright law.

5.2.1 Copyright and Privacy do not Collide

The Berne Convention of 1886 (hereinafter termed “BC”) grants the right of “*public performance*”, of “*communication to the public*” and of “*public recitation*”,⁹⁶ while the WIPO Copyright Treaty of 1996 (hereinafter termed “WCT”) grants the right to make a work available *to the public*.⁹⁷ Considering the wording of these rights, one might argue that the *private* performance, recitation and communication, or the making available, of a work *within the private circle* do not fall within the scope of these rights (hereinafter collectively referred to as “the right of communication”). However, privacy concerns appear not to be the main reason for the creation of this limitation of copyright. Ricketson states it is likely that the term “public” is used to indicate that only communications to “those who are willing to pay for the benefit of hearing or seeing the work performed” should be viewed as restricted acts.⁹⁸ In other words, an economic rationale is at the root of the wording of the Convention. A non-public communication would not affect the interests of the copyright-holder.⁹⁹

The right of communication does not, in effect, penetrate the users’ private sphere because of the addition of the term “public” to the definition of each restricted act. In the definition of the right of reproduction in Art 9(1) of the BC, as well as in national copyright legislation, such an addition is absent. Therefore, private copying would only

⁹² Zimmerman 1992: 686.

⁹³ See Zimmerman 1992: 707. See also Patterson & Lindberg 1991: 179. Of course, protecting the authors’ moral rights is another main goal of copyright, at least in Europe.

⁹⁴ Spoor 1996: 71; Hugenholtz 1996a: 86–87.

⁹⁵ See, eg, Art 15(2) of the German Copyright Act of 1901 (replaced by the Copyright Act of 1965) which stated that to make “a copy for personal use [was] no infringement, if it [did] not have the purpose to derive any profit from the work”. Cited from Reinbothe 1981: n 9. See also Spoor 1996: 72 (observing that small-scale copying for private use was generally considered permissible).

⁹⁶ Arts 11, 11bis, 11ter and 14 of the BC as last revised by the Act of Paris of 1971.

⁹⁷ Arts 6 and 8 of the WCT.

⁹⁸ Ricketson 1987: 432, 453.

⁹⁹ Hugenholtz 1996a: 90.

fall outside the scope of copyright if a specific exemption were applicable. In many continental jurisdictions, private copying by individual users is indeed explicitly statutorily exempted.¹⁰⁰ In the USA, however, a specific statutory exemption does not exist. According to Litman, who observes that many copyright exemptions are the result of multilateral bargaining among affected stakeholders, an explicit private copying exemption is missing because nobody showed up to ask for it.¹⁰¹ Still, however, some commentators presume that private copying falls outside the reach of copyright, either implicitly, following from the structure and principles of copyright law, or because private copying must be regarded as “fair use”.¹⁰²

Whether explicit or implicit, the limitations of national copyright law which allow private copying are based upon Art 9(2) of the BC. This provision permits national legislators to implement exemptions to the right of reproduction “in certain special cases”, if this does not come into conflict with a “normal exploitation of the work” and does not “unreasonably prejudice the legitimate interests of the author”. Although it is not specifically mentioned, and although the criteria in the provision reflect mainly the copyright-holders’ interests, according to Ricketson, private copying is assumed to fall within the scope of the provision. When Art 9(2) was included in the Convention in 1967, it was acknowledged that authors’ rights should not impinge upon what is done in the private sphere. Then, however, most existing legislation that allowed private copying (which the provision was intended to legitimise), was predicated upon the assumption that reproductions would be made by hand or by typewriter. Consequently, it was thought that private copying would not easily affect the normal exploitation of a work or come into conflict with the copyright-holders’ interests.¹⁰³ Concomitantly, the economic interests of the copyright-holder and the users’ right to privacy would not collide.¹⁰⁴

The economic criteria of Art 9(2) of the BC are often expressed in national copyright legislation through the specific prohibition on putting reproductions into circulation which are allowed on the basis of the private copying exemption.¹⁰⁵ Apparently, it is felt that private copies will not interfere with the copyright-holders’ interests as long as they remain within the private sphere. If private copies could be distributed legally, the private copier would directly compete with the copyright-holder. Accordingly, one of the factors

¹⁰⁰ For France, see Act on Intellectual Property of 1992, Art L 122-5, 2; for Belgium, see Copyright Act of 1994, Art 22 § 1, 4; for the Netherlands, see Copyright Act of 1912, Art 16b; and for Germany, see Copyright Act of 1965, § 53.

¹⁰¹ Litman 1997b: text near n 21. Other parties, such as libraries and educators, were present at the negotiations and were rewarded with specific exemptions to their advantage.

¹⁰² Patterson & Lindberg 1991: 193–197. The fair use doctrine is codified in s 107 of the US Copyright Act of 1976 (§ 107 of Title 17 of the USC).

¹⁰³ Ricketson 1987: 485.

¹⁰⁴ Although, for reasons of brevity and clarity, we do not address neighbouring or performers’ rights, it should be noted that Art 15(1)(a) of the Rome Convention of 1961 grants full discretion to the Contracting Parties to treat any “private use” as non-infringing. This provision has been superseded, however, by Art 16 of the WIPO Performances and Phonograms Treaty of 1996, which contains the same criteria as Art 9(2) of the BC. See Ficsor 1997: 214–215.

¹⁰⁵ For the Netherlands, see Copyright Act of 1912, Art 16b(5); for Germany, see Copyright Act of 1965, Art 53(5).

to be considered under the fair use doctrine in the United States is the “effect of the use upon the potential market for or value of the copyrighted work”.¹⁰⁶

5.2.2 Privacy Considerations in Copyright Law

Although privacy considerations did not play – certainly at the international level – an important role in shaping copyright law, it seems that, almost by chance, copyright law was kept out of the users’ private sphere. Communications within the private sphere and private copying were not regarded as significantly denigrating the interests of copyright-holders because these acts were not economically significant.

However, with the emergence of modern audio- and video-recording techniques, the view on private copying changed. Individuals were able easily to make exact copies in the intimacy of their homes. It is not hard to see that this practice could come in conflict with the normal exploitation of the copyrighted works or the interests of copyright-holders.¹⁰⁷ Thus, even though the private copier did not directly compete with the copyright-holder, it was argued that home taping fell under the exclusive right of reproduction and that unauthorised home taping would therefore constitute an act of infringement. To enforce their rights, however, copyright-holders would have to violate the right to privacy of the home.¹⁰⁸ Hence, the exercise of copyright began to conflict with the users’ right to privacy. This collision of rights is addressed in several decisions of the German Federal Supreme Court (*Bundesgerichtshof* – GFSC).

In 1955, in view of the large profits lost through home taping, the GFSC was of the opinion that home audio recording was not covered by the statutory exemption for private copying because it dated from 1901, and at that time the legislator could not have foreseen the technological developments leading to vast amounts of private copies being made.¹⁰⁹ Consequently, even though it seemed covered by the wording of the provision,¹¹⁰ this type of private copying was considered to be an infringement. The Court added that, where the copyright-owners’ interests collide with the privacy interests of the user of a work, the first must prevail, since, without the author’s creative labour, the work would not have been available for copying in the first place. Therefore, a right to prohibit private recordings was granted. The decision was heavily criticised by many commentators. They argued that the legislators had foreseen copying by mechanical devices. Moreover, in their view, even if the legislators had not foreseen this type of copying, it was implicit from the structure of copyright law that the legislators intended copyright not to invade the users’ private sphere. They found that the GFSC had attached too little importance to the users’ personality rights, and particularly to their right to privacy.¹¹¹

¹⁰⁶ Title 17 of the USC, § 107(4).

¹⁰⁷ Davies 1984: 71.

¹⁰⁸ Stewart & Sandison 1989: 83.

¹⁰⁹ GFSC, 18.5. 1955, *GRUR* 1955/10: 492 (*Tonband*).

¹¹⁰ See note 95 above.

¹¹¹ See Haeger 1962, Hefermehl 1957 and Spitzbarth 1963: 882. Spitzbarth refers to several other authors who were of this view.

In 1964, the GFSC brought its 1955 ruling and the opinions of its critics into conformity with each other. It decided that, although home taping indeed constitutes an infringement of copyright, to invade user privacy while *enforcing* copyrights was barred by the constitutionally guaranteed inviolability of the home pursuant to Art 13 of the Basic Law of 1949 (set out in section 1.4.4 above).¹¹² The German collecting society (GEMA) could not demand, therefore, that retailers of recording equipment have buyers of the equipment identify themselves in order to enable GEMA to control whether they had acquired a license to make private copies, because such control would only be possible by penetrating the private homes of the users. Additionally, it would be impossible to enforce copyrights against individual users anyway. Similarly, in 1983, the Court found that an owner of a copy shop could not be obliged to monitor every copy made by his customers, because such control would conflict with the customers' constitutionally granted general privacy rights in Arts 1 and 2 of the Basic Law (set out in section 1.4.4 above),¹¹³ and because such control would be impossible in practice.¹¹⁴

In accordance with these decisions, the German legislators considered that granting a right to prohibit home taping would not be appropriate because of, *inter alia*, privacy concerns, and instead implemented in 1965 a statutory right to equitable remuneration through the imposition of a levy on the sale of sound-recording equipment.¹¹⁵ Similarly, a levy on reprography equipment was introduced in 1985. Thus, the interests of the copyright-holders and the users' right to privacy may be considered to be balanced and user privacy is, albeit indirectly, addressed in copyright law. Many countries have comparable regimes,¹¹⁶ which are often inspired by the German experience.¹¹⁷ In several other jurisdictions, home taping is left totally outside the scope of copyright.¹¹⁸

¹¹² GFSC, 25.5.1964, *GRUR* 1965/2: 104 (*Personalausweise*). The Court stated: "Soll die Namensübermittlung für die Kl. überhaupt einen durchgreifenden Sinn haben, so kann dies nur der sein, daß die Kl. auf Grund ihrer Kenntnis von Namen und Anschriften der Geräteerwerber in deren persönlicher häuslicher Sphäre Kontrollmaßnahmen durchführen und auf diese Weise etwaige Rechtsverletzungen ahnden will. Da die Art der Verwendung der Geräte nur an Ort und Stelle festgestellt werden könnte und die Kl. bereits die Möglichkeit angekündigt hat, die erforderlichen Feststellungen auf Mitteilungen von Wohnungsnachbarn, Portiers usw. hin zu veranlassen, würde hierdurch die Gefahr unangemessener Eingriffe in die Unverletzlichkeit des häuslichen Bereichs heraufbeschworen (Art. 13 GG)".

¹¹³ As shown in section 1.4.4, the German Federal Constitutional Court has found that a person's right to informational self-determination derives from the same constitutional provisions.

¹¹⁴ GFSC, 9.6.1983, *GRUR* 1984/1: 54 (*Kopierläden*). The Court held: "Mit Recht hat jedoch das BerG ausgeführt, daß eine solche generelle Kontrollpflicht im allgemeinen durchgreifenden Bedenken begegnet. Es weist darauf hin, daß die Fotokopiergeräte der Bekl. auch zur Vervielfältigung privater Aufzeichnungen, Urkunden und dergleichen benutzt werden, deren Inhalt vielfach vertraulich und nicht zur Kenntnisnahme durch dritte Personen bestimmt ist. Eine umfassende Kontrolle - und nur sie käme überhaupt als eine wirksame Maßnahme in Betracht - würde den Anspruch des einzelnen Kunden auf Vertraulichkeit, der seine Grundlage in den verfassungsrechtlich geschützten persönlichen Freiheitsrechten (Art. 1, 2 GG) hat, in unerträglicher Weise beeinträchtigen."

¹¹⁵ Haeger 1962: 68-69; see also Reinbothe 1981 and Visser 1997: 48. Additionally, a levy on audio and video tapes was imposed in 1985.

¹¹⁶ In almost all European countries, a comparable regime has been adopted with regard to home taping, except in the UK, Ireland, Sweden and Luxembourg. See Visser 1996: 209.

¹¹⁷ In the Netherlands, for example, the creation of the home taping regime is considered to be based on the protection of the users' private sphere. See Spoor & Verkade 1993: 189.

¹¹⁸ In the UK and the USA, for instance, the copyright-holder has neither the right to forbid the private reproduction of a work nor a right to equitable remuneration. In the USA, home taping to analogue formats

Even though the BC does not provide that communications within the private circle fall outside the ambit of copyright, the copyright legislation of many countries specifically states that an author may not object to the communication of his work within the “family” or “private” circle.¹¹⁹ A decision by the Dutch Supreme Court indicates that the purpose of such provisions is to ensure that copyright does not invade the users’ privacy. According to the Court, the Dutch legislators included such a provision because the author’s protection is intended to be limited by the freedom of the individual citizen.¹²⁰ Consequently, it could be argued that privacy concerns are at the root of this limitation of copyright, at least in some national copyright laws. According to Visser, it is not a coincidence that the sphere protected by the right to privacy is more or less similar to the sphere kept outside the reach of the right of communication. Therefore, this boundary of copyright would not only be the result of practical or economic considerations, but also of a choice of principle.¹²¹

Theoretically, a problem comparable to the one addressed by the German courts in the context of the right of reproduction could exist if a right of communication within the private circle were granted; copyright-holders would have to invade the private sphere of the users to be able to detect infringements and to enforce copyrights. With regard to private performances and recitations, again it would be the right of inviolability of the home which could stand in the way of enforcement of copyrights; with regard to (on-line) communications within the private circle, it could also be the privacy of communications – which is expressly guaranteed by many national constitutions in Europe and by Art 8 of the ECHR (see section 3 above) – which could bar the monitoring and effective enforcement of copyright.¹²² The latter right plays a prominent role in the current discussion on intermediary liability. An argument in this controversy is that to impose a duty of care regarding third-party material would imply the monitoring of the communications facilitated by the intermediary and thus violate the right to privacy of communications which the state is constitutionally obligated to protect. If an intermediary is not allowed to monitor the contents of the messages it disseminates, it can hardly be

is considered “fair use”. Home taping to digital formats apparently is not; a levy is imposed on digital audio tapes and recorders. See Visser 1996: 210. The District Court in the *Betamax* case considered that Congress did not find protection of copyright-holders’ rights over reproduction of their works was worth the privacy and enforcement problems which restraint of home-use recording would create. The Supreme Court, however, did not refer to any privacy concerns in its decision to consider home taping for the purpose of time shifting as “fair use”. The basis for its decision appears to be merely economic. See *Universal City Studios, Inc., v. Sony Corp.*, 480 F Supp 429, 444 (CD Cal 1979), rev’d, 659 F 2d 963 (9th Cir 1981), rev’d, 464 US 417 (1984). Nimmer asserts that the District Court’s reasoning is far from flawless. See Nimmer & Nimmer: 2:8B.12–8B-25.

¹¹⁹ For France, see Act on Intellectual Property of 1992, Art L 122-5, 1; for Belgium, see Copyright Act of 1994, Art 22 § 1(3); for the Netherlands, see Copyright Act of 1912, Art 12(4); for the USA, see Copyright Act of 1976, s 101(1); and for Germany, see Copyright Act of 1965, § 15(3).

¹²⁰ Dutch Supreme Court, 1.6.1979, *NJ* 1979, 470.

¹²¹ Visser 1997: 133; see also Haeger 1962: 52–53. Lucas emphasises that the term “family circle” under copyright law is a narrower concept than the notion of “private”, for the purpose of applying the right to privacy of communications. The first requires some kind of familiarity, whereas the latter applies to any non-public communication. See Lucas 1997: 232

¹²² Visser 1997: 34.

expected to know of those. Thus, it would be unreasonable to impose a duty of care regarding third-party material upon on-line intermediaries.¹²³

5.3 Copyright vs. Privacy in the Digital World

When, with the emergence of home taping and reprography, copyright hesitantly took its first steps into the users' private sphere and thus outgrew the stage of merely protecting against direct competitors, copyright and user privacy were balanced in a way that did justice to both sides; even though copyright slipped into the users' private sphere, the copyright-holder was kept outside of this sphere. In the digital environment, however, legislators appear not to attach much weight to the users' right to privacy; copyright bluntly strides into the private sphere of users. Instead of granting a right to exercise control over acts of commercial exploitation, a right to control the use of works is awarded. Moreover, the application of a levy scheme to balance both rights is, or may be, expressly prohibited.

5.3.1 Computer Programs and Databases

Until recently, copyright-holders had no legal action against the private "consumption" of copyrighted works. To read an unauthorised copy or to view an illegal broadcast would not be restricted acts under copyright law. In the analogue environment, copyright-holders had to exercise their control at the level of exploitation – ie, the reproduction, distribution and public dissemination level.¹²⁴ This situation has changed with regard to software and databases. In Art 4(a) of the EU Software Directive,¹²⁵ temporary reproduction is expressly included among the restricted acts. Therefore, acts which are necessary to use or "consume" software, such as the loading, running, transmitting and displaying of the software, are covered by copyright law, because, with the current state of technology, they require a temporary copy being made in the computer's random access memory (RAM). Similarly, under the copyright protection and *sui generis* right granted in Arts 5(a) and 7 of the EU Database Directive,¹²⁶ the temporary reproduction and "transfer" of a substantial part of the contents of a database are restricted acts. To gain access to an electronic database implies a temporary transfer to, or reproduction in, a computer's RAM. Thus, the private use of a database may be forbidden by the copyright-holder.

The broadening of the right of reproduction may affect the users' "privilege" to communicate privately a work. To make a work perceptible, even in the private circle, is, in effect, covered by the right of reproduction, as is the private on-line communication of the work. These regimes do not simply provide for a right of reproduction or a right of communication to the public aimed, in turn, at granting a right to exercise control at the

¹²³ See Institute for Information Law 1997b: 18–21 and 79–81.

¹²⁴ Litman 1997a: 601; Patterson & Lindberg 1991: 193; Nicholson 1995: 168.

¹²⁵ Directive 91/250/EEC of 14.5.1991 on the legal protection of computer programs (OJ No L 122, 17.5.1991, 42).

¹²⁶ Directive 96/9/EC of 11.3.1996 on the legal protection of databases (OJ No L 077, 27.3.1996, 20).

exploitation level (as copyright traditionally did); they provide for a right to control the *use* of the works concerned.¹²⁷ Furthermore, the possibility for EU Member States to implement an exemption for the purpose of private use of electronic databases is specifically excluded under the Database Directive,¹²⁸ just as it is forbidden under the Software Directive to provide for a private copying exemption to the broad right of reproduction.¹²⁹ Thus, the application of an equitable remuneration scheme, comparable to the home taping or reprography regimes, is impossible under both Directives.¹³⁰ Under either Directive, however, it is provided that the “lawful” user does not need express authorisation to use the product “in accordance with its intended purpose”.¹³¹ This, however, is not equivalent to a private use exemption, since the latter would be applicable independently of how the user acquired the original copy and of what is to be considered the “intended purpose” of the program or database. Also, the “lawful acquirer” of a computer program is statutorily allowed to make a “back-up copy”.¹³² This differs from a general private copying exemption, because the latter could apply to the broadened right of reproduction as well, and because the back-up copy must serve as a replacement, whereas the private copy may serve for any non-commercial private purpose.

While the home taping regime was implemented, at least partly, because it was considered undesirable to have the copyright-holder invade the users’ private sphere, the copyright-holder may now statutorily hold the “unlawful” private user of a computer program or database accountable; ie, the right-holder may now control the private use of these types of works. Apparently, there are no major objections to invading user privacy to enforce rights attached to software or databases; by definition, the interests of the copyright-holders seem to outweigh the users’ right to privacy. To our knowledge, on the other hand, a private individual has never yet been sued for the non-commercial, but copyright-infringing, private use of software.¹³³ A possible reason for this is the great

¹²⁷ Hugenholtz 1996a: 93; see also Spoor 1996: 75. Spoor is of the opinion that the reproduction right had to be broadened in respect of software, because, given that one server may serve a whole battery of computers, the impact of loading a program in RAM would be so great that it must be covered by copyright. Visser, on the other hand, feels that it would be enough if the copyright-holders were able to exercise control over the making available of a copyrighted work on the server. See Visser 1997: 176–177. Litman argues that a “right of commercial exploitation” should be granted instead of a “right to use”. See Litman 1997b: part VI.

¹²⁸ See Arts 5 and 7 of the Database Directive.

¹²⁹ Articles 5 and 6 of the Software Directive are interpreted as providing an exhaustive enumeration of permitted exemptions. Private use is not one of those. See also paras 5.6.17 and 5.8.2(f) of the *Green Paper on Copyright and the Challenge of Technology*, Brussels, 7.6.1988, COM (88) 172 final. There it is observed that instead of providing for a private copying exemption, it would be more appropriate to allow the legitimate user to make back-up copies without authorisation. The pros and cons of a private copying exemption with regard to software are considered. However, end-user privacy is apparently overlooked. The fact that “genuine private copying” is made unlawful is considered to be a side effect which is taken for granted, as it would be impossible to police such copying anyway.

¹³⁰ Hugenholtz 1996b: 133.

¹³¹ Admittedly, this is a simplification. This is not the place, however, to discuss this issue thoroughly. See Arts 5, 6 and 9 of the Software Directive and Arts 6, 8, 9 and 15 of the Database Directive.

¹³² See Art 5(2) of the Software Directive.

¹³³ Litman observes that the suing of non-commercial private users of any type of work is a rarity. See Litman 1997b: near n 49. Of course, infringing private use of a database has never been challenged on the basis of the Database Directive in court either – the Directive is too recent for such a challenge to have been mounted.

difficulty of detecting copyright infringements that occur in the private sphere.¹³⁴ Due to electronic copyright management systems, this may change in the near future. Indeed, the Database Directive seems to anticipate the existence of technological measures which protect copyrighted works and enable direct licensing with each end-user.¹³⁵

In the USA, the approach with regard to software is largely similar. Temporary reproductions in RAM may be covered by copyright.¹³⁶ Section 117 of the US Copyright Act of 1976 states, however, that the “owner” of a copy of a computer program may make a copy of the software provided that it is “created as an essential step in the utilization” of the program. The “owner” is understood to be the “legitimate holder”. The copies must be made only for an owner’s personal use.¹³⁷ The main difference with respect to the European software regime appears to be that the fair use exemption is not blocked in the USA, while the general private copying exemption is blocked under the EU Software Directive. Non-commercial use by consumers, even if inconsistent with the intent of the author, is presumed to be “fair” in the United States.¹³⁸ To our knowledge, however, the fair use defense has never been applied to exculpate private use by a non-legitimate holder of a copy of a program.

5.3.2 Copyright Directive Proposal

In Art 2 of the EU’s Copyright Directive Proposal (CDP),¹³⁹ the temporary reproduction of any type of work is to constitute a restricted act under copyright. Thus, the “consumption” or use of any digitalised work would fall within the scope of copyright law. In Art 5(1) of the CDP, however, it is stated that acts of reproduction “which are an integral part of a technological process for the sole purpose of enabling use to be made of a work” must be exempted in national copyright law. Therefore, contrary to the database and software regimes, broadening the right of reproduction here would not, in principle, enable copyright-holders to exercise copyrights against private users. It is added, however, that this mandatory exemption would apply only when the reproduction has “no

¹³⁴ To cope with this problem the Business Software Alliance introduced an “Anti Privacy Hotline” where software piracy may be reported. See Visser 1997: 57–58. See also <http://www.nopiracy.com>. In the Dutch House of Representatives (*Tweede Kamer*) the legality of the initiative was discussed. The Minister of Justice found that it may possibly be unlawful to elicit the disclosure of information concerning private use. It would be up to the courts to decide. See *Tweede Kamer* 1995-1996, *Aanhangsel* nr. 927.

¹³⁵ Hugenholtz 1996b: 133.

¹³⁶ First decided in *MAI Sys Corp v Peak Computer, Inc*, 991 F 2d 511 (9th Cir 1993), cert denied, 126 L Ed 2d 640, 114 S Ct 671 (1994). See however Nicholson 1995: 167–169 (arguing that the court’s decision is incorrect, because granting a “right to use” software goes beyond what was proposed by the National Commission on New Technological Uses (CONTU), which contemplated a revenue stream on the proliferation of permanent copies, not on the basis of use of computer programs)

¹³⁷ See *Aymes v. Bonelli*, 47 F 3d 23, 26 (2d Cir 1995) where the court followed CONTU, which had stated that the intent of s 117 is to provide a legitimate holder of a computer program with permission to copy the program so that he/she may use it.

¹³⁸ Olson 1992: 909.

¹³⁹ Commission of the European Communities, *Proposal for a European Parliament and Council Directive on the Harmonization of certain Aspects of Copyright and related Rights in the Information Society*, Brussels, 10.12.1997, COM(97) 628 final. Available at URL <http://europa.eu.int/comm/dg15/en/intprop/intprop/1100.htm>.

economic significance”. Consequently, the exemption is not absolute; an economic criterion would determine its applicability. If certain uses that require temporary reproductions are considered economically significant, an exclusive right to *use* copyrighted works privately may be granted on the basis of the proposed Directive. It is difficult to predict when use will be considered economically significant. The software and database examples could imply, however, that this hurdle is not too difficult to clear.¹⁴⁰

Although the Explanatory Memorandum to the CDP acknowledges that, in the context of home taping, it is “not even desirable to enforce an exclusive right in this area of private use for reasons of privacy”,¹⁴¹ end-user privacy is not specifically treated as a factor of importance in relation to digital use. Instead, in conformity with Art 9(2) of the BC, the Commission seems to take mainly the copyright-holders’ economic interests into account. This becomes even more apparent when one considers that, in Art 5(2)(b) of the CDP, a limitation “in respect of reproductions on audio, visual or audio-visual recording media made by a natural person for private use and for non-commercial ends” is included only on an optional basis. From the CDP’s Explanatory Memorandum, it can be concluded that this exemption has not been made mandatory, because it is expected that digital technology will be available in the future which will “allow the effective control of private copying and the replacement of levy schemes by individual licensing solutions” (ie, pursuant to electronic copyright management systems).¹⁴² According to the Commission, the major reason for applying the private copying exemption to home taping is the practical impossibility of enforcing copyrights against individual private users.¹⁴³ Apparently, it would be appropriate that EU Member States abolish private copying exemptions for digital reproductions when electronic copyright management systems become available.¹⁴⁴

5.4 Technological Measures vs. Privacy

In sum, private use of digital works would seem to be brought within the copyright-owners’ sphere of control because of its economic significance, and because, contrary to the enforcement of private analogue use, the enforcement of private digital use through an ECMS is presumed not to conflict with the users’ right to privacy. In any case, the issue is not expressly addressed. The impossibility of enforcing copyrights against individual users is viewed to constitute the main reason for private copying exemptions. Until now, the effect of enforcing, through an ECMS, “digital” copyrights within the

¹⁴⁰ It is not unlikely that technologies will soon exist that make a work disintegrate when it is accessed a fixed number of times. Then, each temporary reproduction that occurs while the work is accessed may be viewed as having economic significance. See Litman 1997a: 601.

¹⁴¹ See Comment 4 in Chapter 3, Part I A.

¹⁴² See Comment 6 with respect to Art 5. Another reason for abolishing private copying exemptions may be that they could be applicable to temporary reproductions. Then, even if the exemption in Art 5(1) of the CDP were not applicable, a temporary reproduction for the purpose of private use might not constitute an infringement on the basis of the general private copying exemption.

¹⁴³ See Comment 4 in Chapter 3, Part I A.

¹⁴⁴ The Danish Copyright Act of 1995 already excludes from the private copying exemption the making of a digital copy of subject matter incorporated in digital media. See Schoning 1998: 178.

private sphere has been merely a theoretical issue; even if copyright-holders were granted the right to exercise control at the level of the individual private user, they were unable to enforce their broadened right in practice. In the near future, however, an ECMS may enable them to monitor private usage and enforce copyright against any individual user. This may not only impinge upon the users' right to informational privacy, also the users' private sphere could be invaded, albeit electronically. One option to cut back on this potential would be to block private use through the construction of "electronic fences" that the end-user cannot cross. These sorts of technological measures are briefly investigated below.

5.4.1 Monitoring

New techniques currently under development would enable the copyright-holder to monitor easily the use of his/her/its work and to detect copyright infringements and violations of license terms even in the users' private sphere. Some techniques would depend on a software module attached to a digitalised copy of the work which is disseminated on-line. The module would record everything that happens to the copyrighted material. Each time the work is used, the module would send a message to the copyright-owner, thus providing him/her/it with an audit trail.¹⁴⁵ The licensor would then be able to bill the user for each specific use, or spot violations of the terms of the license. Obviously, the data must be processed in accordance with data protection regulations. But not just informational privacy may be violated, so too may the more general right to privacy. Even though such electronic monitoring is more subtle than a physical search-and-seizure procedure, from the above-mentioned decisions of the German Federal Supreme Court could follow that penetrating into users' domestic or private sphere by such monitoring may be barred by the users' right to privacy. This would especially be the case if alternative, less privacy-invasive solutions are available. The availability of such solutions was one of the reasons why the GFSC did not acquiesce to GEMA's demand in 1964.¹⁴⁶

Although the monitoring of non-commercial private use of copyrighted works to control whether the terms of license are observed is unprecedented, it is an established practice in the context of pay-per-view television to bill the viewer for each actual use of the service. By paying a subscription fee, the customer gains access to the program. The system does not stand in the way of taping the program and reviewing it countless times, or even of sharing a copy within a private circle. The above-mentioned monitoring technique would go a step further. Even after the purchase of a copy, the copyright-holder would keep sight of each private use made of a work. Interestingly, legislators in the USA felt it was necessary to protect specifically the informational privacy of subscribers

¹⁴⁵ Clark 1996: 143; See also Cohen 1996: n 10.

¹⁴⁶ The GFSC considered that the imposition of a levy scheme, such as existed with regard to public performances, would provide an alternative solution. In this case, the principle of proportionality was applied in the context of what could be considered "zumutbar" (ie, what could reasonably be expected of the defendants to avoid endangering the rights of others). See more extensively Institute for Information Law 1997b: 14–16. The criterion of proportionality also applies under Art 8 of the ECHR: see section 3 above.

to cable services in the Cable Communications Privacy Act of 1984, which is applicable to pay-per-view services. The Act allows the collection of personally identifiable information to detect unauthorised reception of the cable communications. Still, however, it is only the unauthorised first access that can justify an intrusion of the right to privacy, and not the occurrence of private copying or the private communication of the work.

5.4.2 Blocking

Another technological measure to protect copyrighted works would be to encrypt copyrighted material and thus block access to such works, or certain uses of them, unless an access key is acquired. Thus, copyright and compliance with the terms of a license could be effectively enforced, even without the licensor having to obtain knowledge of the actual use that is made of a work. If no personal data are acquired or disclosed, there can be no violation of data protection laws, and the only aspect of the right to privacy which might be breached is the right to the privacy of the home – ie, the copyright-owner could be viewed as “blindly trespassing” into the users’ private sphere. Mackaay observes that technological blocking measures could be compared to fences protecting real property.¹⁴⁷ In this case, the measures could be viewed as negatively “fencing in” the users’ private sphere. The above-mentioned analogy is perhaps not entirely accurate (as analogies rarely are),¹⁴⁸ and somewhat far-fetched. It may be more accurate to say that a measure like blocking will constrict user *autonomy*. Certainly, such a measure will interfere with the users’ autonomy more than copyright traditionally has done. For example, a multimedia product could be designed to prevent the making of print-outs, thus blocking the reproduction for private, non-commercial purposes.

Some commentators assume that private copying exemptions are particularly aimed at protecting the individual’s private sphere.¹⁴⁹ The German copyright scholar, Kohler, saw a connection between the ability to copy for private, non-commercial purposes and the freedom of thought.¹⁵⁰ Moreover, when Art 9(2) was inserted into the Berne Convention, the normative position was taken that copyright should not impinge on what is done in the private sphere.¹⁵¹ If the intention of the private copying exemptions is to have neither copyright nor the copyright-holders interfere with user privacy or autonomy, the question may be posed whether it is desirable that private uses be effectively blocked by copyright-holders as soon as the work concerned is used in the digital environment. From a strictly privacy perspective, however, blocking seems preferable to the monitoring of private use.¹⁵²

¹⁴⁷ Mackaay 1996.

¹⁴⁸ See Litman 1997b: near note 42. Litman rightly observes that analogies are often misappropriated in assessing the effects of regulations in the digital environment.

¹⁴⁹ Hugenholtz 1996a: 94; Hefermehl 1957: 65; Haeger 1962.

¹⁵⁰ See Spoor 1996: 73–74; see also Cohen 1996: Part IV. Cohen argues that the close interdependence between the receipt and expression of information, and between reading and freedom of thought, would make recognition of a right of anonymous access to reading materials “sound constitutional policy”. Note too the Proceedings of the First IMPRIMATUR Consensus Forum 1996: 86 (agreeing that user privacy is closely related to the freedoms of expression, association and assembly).

¹⁵¹ See section 5.2.1 above.

¹⁵² See also Cohen 1997: 185.

5.5 Statutory Protection of Technological Measures

On top of the protection provided by copyright, contract law and technological measures, copyright-owners have been deemed to need an additional layer of protection in the digital environment: this being the legal protection of technological measures intended to protect copyrighted works.¹⁵³ In the following, we examine whether the legal protection schemes that are adopted or proposed for this purpose are in line with the balance between copyright and the users' right to privacy which exists under "analogue" copyright law. In other words, we consider whether tampering with the above-mentioned technological measures for the purpose of private, non-commercial use of copyrighted works or of safeguarding user privacy, is outlawed.¹⁵⁴

The WIPO Copyright Treaty (WCT) was signed in 1996.¹⁵⁵ The Treaty is intended to supplement the Berne Convention. Articles 11 and 12 of the Treaty oblige the Contracting Parties to provide legal protection for ECMSs.¹⁵⁶ Article 11 states:

Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law.

Clearly, the act of circumventing technological measures by an end-user is covered by the provision.¹⁵⁷ However, by its wording, Art 11 of the WCT only applies to measures that "restrict acts ... not ... permitted by law". If private copying as well as communicating within the private circle are permitted under copyright law, the Contracting Parties would not have to provide for legal remedies against the circumvention of technological

¹⁵³ The first example of such legal protection in European law is Art 7(1)(c) of the Software Directive which obliges EU Member States to provide remedies against "any act of putting into circulation, or the possession for commercial purposes of, any means the sole intended purpose of which is to facilitate the unauthorized removal or circumvention of any technical device which may have been applied to protect a computer program". The first precedent for legal protection of technological measures that prevent certain uses of copyrighted works in the USA can be found in the Audio Home Recording Act of 1992 (§ 1002, Title 17 of the USC). The Act obliges manufacturers, importers and distributors of digital audio recording devices to include a "serial copyright management system" (SCMS) in any distributed digital audio recording device. An SCMS would make it impossible to copy from copies. To copy from the original would not be hampered by such a system. The Act also forbids the distribution of devices that would enable circumvention of the system or to perform services the purpose of which is to circumvent an SCMS. See Nimmer & Nimmer: 8B-5-8B-51.

¹⁵⁴ Cf Cohen 1996: Part V (arguing that anti-tampering provisions which are contrary to fundamental rights would not be constitutional and, thus, not enforceable).

¹⁵⁵ Available at URL <http://www.wipo.org/eng/diplconf/distrib/94dc.htm>.

¹⁵⁶ In Arts 18 and 19 of the WIPO Performances and Phonograms Treaty of 1996, similar provisions are included with regard to neighbouring rights.

¹⁵⁷ Note Art 13 of the *Basic Proposal for the Substantive Provisions of the Treaty on Certain Questions Concerning the Protection of Literary and Artistic Works to be Considered by the Diplomatic Conference of 30.8.1996* (WIPO CRNR/DC/4): this would have made unlawful not the act of tampering itself but the manufacturing, distribution and possession of devices that enable circumvention. Thus, circumvention for private purposes would not have been covered. Moreover, note 13.05 stated that the Contracting Parties could take into consideration "the need to avoid legislation that would impede lawful practices".

measures for the purpose of performing these acts. Moreover, because the provision mentions “law” in general, and not copyright law in particular, it would seem that even the circumvention of technological measures to perform acts that are not permitted under copyright law itself, but permitted on the basis of other areas of the law (eg, the rights to privacy or freedom of expression), may be allowed.¹⁵⁸

According to a WIPO document, Arts 11 and 12 of the WTC were inserted because it was felt that in a digital environment “no rights may be applied efficiently without the support of technological measures of protection and rights management information necessary to license and monitor uses”, and that appropriate legal provisions were needed to protect the use of such measures and information.¹⁵⁹ Apparently, measures which are designed to *monitor* the uses of copyrighted works are intended to fall within the scope of the provisions, even though the monitoring of the use of a work does not necessarily “restrict acts”, and, hence, does not seem to be covered by Art 11 of the WTC. Moreover, monitoring may be contrary to the users’ right to privacy. Because the act of circumvention may be allowed on the basis of the law in general, it would seem that the provision could be interpreted as permitting the Contracting States not to outlaw the circumvention of technological measures the purpose of which is to monitor the private use of copyrighted works, if such monitoring would collide with the right to privacy.

In Chapter III of the CDP, the European Commission establishes the framework within which EU Member States would have to implement the WCT. Article 6 of the proposed Directive sets out the Member States’ obligations regarding technological measures:

Member States shall provide adequate legal protection against any activities, including the manufacture or distribution of devices or the performance of services, which have only limited commercially significant purpose or use other than circumvention, and which the person concerned carries out in the knowledge, or with reasonable grounds to know, that they will enable or facilitate without authority the circumvention of any effective technological measures designed to protect any copyright or any rights related to copyright as provided by law or the *sui generis* right provided for in Chapter III of the European Parliament and Council Directive 96/9/EC [ie, the *sui generis* right granted in the Database Directive].

It is not entirely clear from the wording of the provision if it is proposed to outlaw the act of circumvention as such. From the CDP’s Explanatory Memorandum, however, it can be concluded that the act of circumvention is meant to be covered by the provision, although, in conformity with copyright tradition, it is stressed that the real danger for intellectual property rights will not be the single act of circumvention by individuals.¹⁶⁰

Due to the definition of “technological measures” in Art 6(2) of the CDP, only devices designed to prevent or inhibit the *infringement* of copyright or related rights must be legally protected. Therefore, the circumvention for the purpose of non-infringing uses of copyrighted works, such as the making of private copies, or the communication within the private circle, will still be allowed, except where a reproduction for private purposes

¹⁵⁸ See also Cohen 1997: 176.

¹⁵⁹ *WIPO National Seminar on Digital Technology and the New WIPO Treaties* (WIPO/CNR/SER/97/1), 7.

¹⁶⁰ See the comments with respect to Art 6.

is made of a database or computer program.¹⁶¹ If the private copying exemption were abolished with regard to other types of works, and the temporary reproduction were regarded as a restricted act because of its economic significance,¹⁶² then the circumvention of technological measures by individuals to enable private copying or uses which require an ephemeral reproduction being made, would be outlawed as well.

Although end-user privacy does not appear to have been a factor of importance when the Commission considered the scope of copyright, the Commission is aware that enforcing copyrights through an ECMS may come into conflict with the users' right to privacy. The CDP's Explanatory Memorandum states:¹⁶³

Since technological identification and protection schemes may, depending on their design, process personal data about consumption patterns of protected subject matter by individual consumers and thus may allow for tracing of on-line behavior, it has to be ensured that the right of privacy of individuals is respected. Therefore, such technological measures must incorporate in their technical functions privacy safeguards in accordance with the Data Protection Directive.

When Clark stated that "the answer to the machine is in the machine", he thought of the answer to the threat to the copyright-holders' interests posed by the use of copyrighted works in the digital environment.¹⁶⁴ Now the Commission places hope on machines to answer the threat that the answering machines pose to the users' right to informational privacy. It is noteworthy that only informational privacy is considered; the general right to privacy (ie, interference with the users' private sphere) is not addressed. It is assumed that the users' informational privacy will be properly protected through the application of PETs. As is shown in section 2.3.1 above, the EU Data Protection Directive allows processing of personal data if it is necessary for the performance of a contract or for the establishment, exercise or defense of legal claims. If these categories are interpreted broadly, the DPD may not protect against the processing of data concerning private use of works that are acquired and licensed through an ECMS. In any case, the DPD does not regulate the way that data are collected, except for the rather vague requirement of fairness in Art 6(1)(a).¹⁶⁵ Whereas the relationship between copyright and privacy is a problem with broad implications,¹⁶⁶ and whereas user privacy and autonomy may be viewed as already addressed in copyright law,¹⁶⁷ the extent to which the users' private sphere may be invaded while enforcing copyrights through an ECMS should arguably not be left to a general regulatory instrument like the Data Protection Directive, but should be

¹⁶¹ Of course, the "lawful user" may statutorily use a computer program "in accordance with its intended purposes". Would the blocking of certain uses determine what will be considered the "intended purpose"?

¹⁶² See section 5.3.2 above.

¹⁶³ See Comment 1 in Chapter 3, Part III A.

¹⁶⁴ Clark 1996.

¹⁶⁵ See section 2.3.1 above

¹⁶⁶ To process data concerning the use of information products may not only have privacy implications. These are *information* products. As Cohen shows, a right to read anonymously may not only derive from the right to privacy but also from the rights to freedom of expression and of association. See Cohen 1996. Moreover, the fact that in the United States (which lacks an omnibus data protection law) informational privacy in the area of video rental, cable communications and library services (see section 2.3.2 above) is specifically regulated, indicates the sensitive nature of data regarding the information one consumes.

¹⁶⁷ See section 5.2.2 above.

addressed more explicitly in copyright law.¹⁶⁸ To what extent should copyright-holders be permitted to process data concerning individual usage of copyrighted works, or to otherwise interfere with the users' private sphere? Do the copyright-holders' interests justify such interference?¹⁶⁹

In legislation pending in the USA – this being the WIPO Copyright Implementation Act (HR 2281), introduced on 29.7.1997, and the Digital Era Copyright Enhancement Act (HR 3048), introduced on 13.11.1997 – the approach appears to be more or less similar to the line taken in Europe. The latter Bill would prohibit the circumvention of technological measures “for the purpose of facilitating or engaging in *an act of infringement*” (emphasis added).¹⁷⁰ Thus, circumvention for non-infringing private purposes would not be covered. The former Bill is less clear in this respect. Measures that protect access to works and measures that protect “traditional” copyright rights are distinguished. The first would be protected through the proposed section 1201(a), which would forbid circumvention of a technological protection measure that “*controls access to a work protected under the Copyright Act*” (emphasis added). Does this mean that circumvention of technological measures for any purpose would be forbidden, as long as the work concerned is the subject-matter of copyright law? If so, tampering for the purpose of gaining access for private use would be outlawed. The proposed provision could also imply that only when the work is actually protected by copyright law – ie, if no exemptions or limitations are applicable – would the act of circumvention in order to gain access be unlawful. The proposed section 1201(b) would aim to protect a measure that “*protects a right of a copyright owner*” (emphasis added). Supposedly, circumvention for the purpose of “fair” private use would not be covered.

5.6 Statutory Protection of Copyright Management Information

The IMPRIMATUR Business Model does not envisage implementing any of the above-mentioned, far-reaching “technological measures”. In the Business Model, the copyright-holders will rely on the monitoring of the works sold through the MD and on the imprint of an identifier of the work, the MD and the work's purchaser. These imprints will facilitate the monitoring of the “flow of works” within the system and could serve as an article of evidence against the purchaser if a licensed work pops up somewhere in violation of the terms of the license. Also, by applying search-engines to search for an imprinted identifier, it would be fairly easy to control whether or not a work is made available on a network. Implementation in national legislation of Art 12 of the WTC would protect imprints of so-called “rights management information” (RMI). RMI is defined as:

¹⁶⁸ See also Cohen 1996: Part VI (“Rather than penalizing legitimate and constitutionally protected individual conduct, the government could enact legislation that would outlaw intrusive, anonymity-destroying practices by copyright owners....”).

¹⁶⁹ Interestingly, Art 60 of the Greek Copyright Act of 1993 specifies that, by decree, the application of mechanisms limiting the use of copyrighted works may be imposed *as long as this does not unjustifiably violate the interests of the users* (emphasis added). See Lucas 1997: n 41.

¹⁷⁰ See the proposed s 1201(a).

information which identifies the work, the author of the work, the owner of any right in the work, or information about the terms and conditions of use of the work, and any numbers or codes that represent such information, when any of these items of information is attached to a copy of a work or appears in connection with the communication of a work to the public.

Neither the imprinted Media Distributor ID nor the Purchaser ID appear to fall within the meaning of any of the enumerated kinds of information. Therefore, these IDs appear not to be covered by the provision. Consequently, if the provision were directly implemented in national legislation, the removal of these imprints or to knowingly distribute or communicate to the public works from which such imprints are removed or altered would not be outlawed.

In Art 7 of the CDP, the EU Member States are required to provide legal protection against any person who removes or alters RMI. The definition of RMI does not include information concerning the purchaser. According to the Explanatory Memorandum for the proposal, Art 7 only “aims at the protection of electronic rights management information, and does not cover all kinds of information that would be attached to the protected material”. Moreover, the provision does not cover removal or alteration that occurs with “authority” – ie, is permitted or even required by law (eg, the EU Directive on data protection).¹⁷¹

Similarly, in the above-mentioned Bills introduced in the US Congress, information regarding the purchaser of a work is not included in the definition of RMI, and user privacy is expressly addressed.¹⁷² In the most recently introduced Bill concerning, *inter alia*, the legal protection of RMI, personal information relating to users of a work is explicitly excluded from the definition of RMI.¹⁷³ Therefore, removal or alteration of such information would not be unlawful.

Apparently, the designers of these RMI protection schemes found that it would be disproportionate in relation to the end-users’ privacy rights to protect imprinted information regarding the purchaser.

5.7 Licenses

One of the purposes of an ECMS is to license directly with each individual end-user. The user would not only obtain an on-line disseminated copy of the work, but also an accompanying license, which would allow certain uses of the work. Thus, not only copyright, but also a contract, would be a legal ground for enforcement. Obviously, to enforce the terms of a valid contract against an individual is possible in any jurisdiction. An argument could then be that it is necessary to know the user and to monitor the actual use of a work in order to control whether the terms of the license are observed. In the EU

¹⁷¹ See explanatory comments 1 and 2 with respect to Art 7.

¹⁷² See, eg, the proposed s 1202(c) of the WIPO Copyright Implementation Act (HR 2281). Subsection 1202(c)(6) would authorize the Register of Copyrights to outlaw by regulation the removal or alteration of other types of information than are enumerated, except for “any information concerning the user of a copyrighted work”.

¹⁷³ See s 1202(c) of the Digital Era Copyright Enhancement Act (HR 3048).

Data Protection Directive, the processing of personal data is expressly allowed if necessary for the performance of a contract.¹⁷⁴ Still, the question remains how far one can go in monitoring the extent to which a contract is observed when this monitoring involves physical or virtual penetration into the purchaser's private/domestic sphere. The 1964 and 1983 GFSC decisions, and the subsequent adoption of the home taping and reprography regimes, can be interpreted to imply that it would go too far to license with each private user of copyrighted works: although copyright may invade the private sphere, the rights holder should stay out of it.¹⁷⁵ On the basis of the 1964 *Personalausweise* decision, it could even be argued that the requirement of user identification so as to enforce copyrights within the individuals' private sphere after occurrence of an infringement, would be disproportionate in relation to the copyright-owners' interests because, in the end, to enforce copyrights, actual private use will have to be monitored, thus invading the users' private sphere.¹⁷⁶ From the European software and database regimes and the Copyright Directive Proposal, however, a conclusion to the contrary could be drawn.

Until recently, copyright contracts were concluded merely between a copyright-holder and a party intending to exploit commercially a copyrighted work. The private use of copyrighted works can hardly qualify as an act of commercial exploitation, although, as the home taping controversy shows, private use could be regarded as conflicting with the normal exploitation of a work or the legitimate interests of the copyright-holder. However, copyright-holders are already contracting with private end-users. It is common practice now to include so-called shrink-wrap licenses with hard copies of computer software or multimedia products. To our knowledge, however, a shrink-wrap license has never yet been enforced against an individual who used the work privately and non-commercially,¹⁷⁷ again probably because it is virtually impossible to detect a violation of the terms of a license which occurs in the private sphere.

If tampering with technological measures to enable private use, or the removal of imprinted information concerning the user, were not declared unlawful, the copyright-holder would have to rely on a contractual obligation of the user to have legal grounds to hold him/her accountable for these acts. If the balance that exists in the analogue world is to be maintained, the question may be asked whether clauses in a license which forbid removal of a purchaser ID or which forbid copyright-circumventing measures for the purpose of private use, should be enforceable. Here the heavily debated issue of the overridability of the limitations of copyright comes into play. Are such licenses pre-

¹⁷⁴ See section 2.3.1 above

¹⁷⁵ Article 29 of the Dutch Copyright Act of 1912 could serve as an illustration of this assertion. It states that seizure of infringing items, which is permitted under Art 28, is not allowed from a person who does not make it a business to trade in the infringing items, and who acquired the items only for private use, unless the person himself infringed copyrights.

¹⁷⁶ See also Proceedings of the First IMPRIMATUR Consensus Forum 1996: 88 (agreeing that a reader should only be identified in a transaction if required by a specific law).

¹⁷⁷ The validity and enforceability of shrink-wrap licenses has been disputed several times. In the USA, see *Vault Corp v Quaid Software*, 847 F 2d 255 (5th Cir 1988); *Step-Saver Data Systems, Inc v Wyse Technology*, 939 F 2d 91 (3rd Cir 1991); *Arizona Retail Systems, Inc v Software Link, Inc*, 831 F Supp 759 (D Ariz 1993); *ProCD, Inc v Zeidenberg*, 86 F 3d 1447, (7th Cir 1996); *Storm Impact Inc v Software of the Month Club*, DC NI11, No 95 C 2154, 9/3/97. For the UK, see *Beta Computers (Europe) Ltd v Adobe Systems (Europe) Ltd* [1996] FSR 367. For the Netherlands, see Rb Amsterdam, 24.5.1996 (1997) *Computerrecht* 63.

empted by copyright law? Can other areas of the law be invoked in court to invalidate these licenses? There are no clear-cut answers to either question.¹⁷⁸

An argument in favour of contractual freedom in this respect could be that consumers are always free not to accept a contract, or to turn to another information provider; market forces would determine whether such limitations and contracts are acceptable to users. In this context, however, it should be considered that copyright, in effect, gives the copyright-holder a monopoly over the work concerned, and that the consumer will usually not be the information-provider's equal in bargaining power.¹⁷⁹ Perhaps, therefore, some kind of consumer protection would be desirable. It would even be possible to go a step further: even if the copyright-holder did not have a legal action against removal or circumvention, most consumers would, in practice, not have the technical ability to perform these acts. Therefore, if the above-mentioned balance should be upheld, it could be argued that the copyright-owners should be forbidden to use technological measures which block or monitor private use or imprint user information in an acquired work.¹⁸⁰

On the other hand, it is unclear in what direction the market will develop. If copyright-holders become unable to receive adequate remuneration due to the vast growth of private, uncontrolled use of copyrighted works, awarding them with a right to exercise control over private use may be considered necessary. Moreover, to be able to pay for each individual, private use of a work may be favourable to consumers, despite the fact that their privacy is invaded. They might, for instance, appreciate customer-tailored services provided through consumer profiles. Furthermore, the losses that copyright-holders currently suffer due to private use are passed on to consumers who do pay for the use of copyrighted works. Bell argues that the application of electronic copyright management systems may therefore lead to a world where information costs less than under the existing fair use doctrine.¹⁸¹ But, then again, perhaps criteria of efficiency and wealth maximisation are not very appropriate to apply where a fundamental right is at stake.¹⁸²

5.8 Maintaining the Balance

If, in order to respect the private sphere of users, communications within the private circle as well as private copying are viewed as left outside the reach of copyright law, the question may be posed whether the emerging possibility to license with each individual user, and to monitor and control the private use of a work, can justify delimiting user privacy by enforcing copyright to a further extent than “analogue” copyright law does. Should privacy, as Geller argues, be given priority over copyright in cases of conflict,

¹⁷⁸ For extensive treatment of these topics, see Institute for Information Law 1997a; Elkin-Koren 1997; Bell 1998: 608–614.

¹⁷⁹ See also Elkin-Koren 1997: 109; Cohen 1996: part III.

¹⁸⁰ See also Cohen 1996: as quoted at note 168 above.

¹⁸¹ Bell 1998.

¹⁸² See also Zimmerman 1992: 713 (arguing that economic theories are a poor source to consult when considering the relationship between freedom of speech and copyright).

since the former is a basic human right intimately connected with the freedom of expression?¹⁸³ A counter-argument could be that copyright promotes freedom of expression as well.¹⁸⁴ In any case, legislators are not only obligated under international copyright law to take the copyright-holders' interests into account, they are also bound by their respective constitutions and by international treaties to protect their citizens' privacy. Neither the right to privacy, nor copyright, nor, for that matter, any property right, is an absolute right.¹⁸⁵ It would seem, therefore, that neither right prevails by definition.

Up until some thirty years ago, and almost by coincidence, copyright and the users' right to privacy did not collide. When it was felt that they did, because of the development of home taping, both rights were nevertheless balanced by imposing a levy on copying equipment and blanket tapes rather than granting a right to prohibit the private copying of copyrighted works. Should this balance be upheld now that circumstances have changed with the development of the digital networked environment? In recital 21 of the Copyright Directive Proposal, the Commission considers that a "fair balance" between copyright-holders and users of protected subject-matter must be safeguarded. A "fair" balance does not have to be similar to the balance achieved in the analogue environment. The peculiarities of the digital environment may mean that the equilibrium should shift to the one or other side. The European software and database regimes, for example, appear to express the need for an extension of copyright to the unlawful private "consumption" or use of copyrighted products in the digital environment, although, to our knowledge, such a broadened right has not yet been invoked to prohibit non-commercial, private use by an "unlawful" acquirer. The CDP would permit EU Member States to abolish the private copying exemption with respect to digital copying of those works not covered by the software and database regimes, and to broaden the right of reproduction to cover the use of these works when such use must be considered economically significant. Apparently, the copyright-holders' interests gain more weight when a work is to be used in the digital environment. However, the users' right to privacy appears to be mostly overlooked when the scope of copyright and the reach of the copyright-holder in the digital environment are considered.¹⁸⁶ Remarkably, user privacy is apparently a factor of greater importance in the context of the legal protection of RMI. The fact that a blind eye is turned to the users' right to privacy where digital use of copyrighted works is

¹⁸³ Geller 1996: 35. See also Proceedings of the First IMPRIMATUR Consensus Forum 1996: 86 (agreeing that, as a general point of departure, a state of privacy is to be preferred rather than a state of no privacy). Note too Cohen 1996 who argues that a "right to read anonymously" may derive, apart from the right to privacy, from the right to freedom of information and expression and the right to associate anonymously.

¹⁸⁴ See Haeck 1998: 35–37.

¹⁸⁵ As noted in section 1.4.4 above, Art 8(2) of the ECHR states, *inter alia*, that the right to privacy may be limited if necessary for the protection of the rights of others. In its *Kirchen- und Schulgebrauch* decision, the German Federal Constitutional Court stated that copyright is a property right and thus protected under Art 14 of the Basic Law of 1949 which allows property rights to be restricted to serve the public interest: see GFCC 7.7.1971, *GRUR* 1972: 481. Similarly, Art 1 of the 1st Protocol to the ECHR (which protects the "peaceful enjoyment" of possessions), provides that a State Party may "enforce such laws as it deems necessary to control the use of property in accordance with the general interest". In the USA, the situation is comparable in this respect: see Cohen 1996: near n 162.

¹⁸⁶ See LAB 1995: under "Human Rights" (noting that informational privacy considerations are practically absent from the Green Paper on Copyright and Related Rights in the Information Society (European Commission 1995)).

concerned seems to follow from a presumption that enforcement through an ECMS will not unduly impinge on the users' private sphere and that the main reason for exempting private copying is the practical impossibility of enforcing copyright against individual users. Even if the latter view is correct, enforcement of copyrights through an ECMS will delimit user privacy and autonomy more than "analogue" copyright does. Given the importance of privacy and freedom of information and expression in a democratic society, and given the fact that copyright, in effect, constitutes a form of information policy, it may be desirable to undertake a careful and explicit balancing of interests to determine the extent to which the users' right to privacy may be disturbed to enforce copyrights through an ECMS.¹⁸⁷

¹⁸⁷ See also LAB 1995: under "Human Rights" ("...the right to privacy and the freedom of expression and information are clearly affected and therefore need careful consideration. The LAB therefore recommends that the Commission give sufficient attention and weight to issues of privacy protection and freedom of expression and information when undertaking any initiative in the area of intellectual property rights in the digital environment.").

6. Conclusion

This study shows that the development of electronic copyright management systems has the potential to impinge on the privacy and related interests of purchasers/users of copyrighted information products to an unprecedented degree. At the same time, various safeguards – legal, technological and organisational – do exist which may reduce this potential. Ultimately, the stringency of these safeguards in practice will be determined by the outcome of interest-balancing processes.

On the legal-ethical plane, the interest-balancing process will mainly consist of an assessment of what is *necessary/proportionate* for ensuring the effective enforcement of copyright-holders' legitimate interests in the light of the privacy and related interests of purchasers/users. On the commercial-political plane, the interest-balancing process will mainly take the form of a struggle between, on the one hand, copyright-holders and their representative organisations and, on the other hand, consumer groups, for the sympathies of legislators.

On both planes, however, the most important thing will be to secure *balanced* and *thorough* public debate about how best to weigh up the above interests. It is undesirable that the outcome of the interest-balancing be determined, in effect, by technological fiat or by one-eyed lobbying. This report may hopefully contribute to preventing such an outcome.

7. Legal SIG Workshop on Privacy, Data Protection, Copyright and ECMSs

On 23 May 1998, an IMPRIMATUR Legal SIG workshop was held on privacy, data protection, copyright and ECMSs at the Institute for Information Law in Amsterdam. The participants discussed the three themes presented below and related issues. It was agreed upon that the statements put forward by the participants would be presented in an anonymous form. Many of the arguments were put forward by a single participant and do not represent a majority opinion. The statements presented below do not necessarily reflect the views of the Institute for Information Law, the IMPRIMATUR consortium or any of its partners. These minutes merely reflect the way the discussions evolved.

The IMPRIMATUR website is: <http://www.imprimatur.alcs.co.uk>

Workshop participants:

Chris Barlas	Authors Licensing and Collecting Society Limited
Jon Bing	Norwegian Research Centre for Computers and Law
Lee Bygrave	Norwegian Research Centre for Computers and Law
Charles Clark	Federation of European Publishers
Julie Cohen	University of Pittsburgh
Ute Decker	Institute for Information-, Telecommunication- and Media Law, Münster
Michael Froomkin	University of Miami
Lucie Guibault	Institute for Information Law
Bernt Hugenholtz	Institute for Information Law
Jan Kabel	Institute for Information Law
Kamiel Koelman	Institute for Information Law
Björn Lindgren	Telia InfoMedia
Eric Luijff	TNO Physics and Electronics
Darrell Panethiere	International Federation of the Phonographic Industry
Alfred Roos	Dutch Department of Justice
Peter Seipel	Swedish Law and Informatics Research Institute
Erik Terheggen	BUMA/STEMRA (CISAC)
Feer Verkade	University of Leyden
Dirk Visser	Stibbe Simont Monahan Duhot

Reporters: Amelia Keuning and Annemique de Kroon

General introduction by Jan Kabel – Privacy, Data Protection and Copyright: Their Interaction in the Context of Electronic Copyright Management Systems

Jan Kabel started his introduction with a loose translation of the first line of a poem by Dutch poetess Neeltje Maria Min:

“ Call me, call me, call my name,
I only want to be called by the one I love”

These lines belong to bygone days since now everybody knows our name: banks, supermarkets, insurance companies, telecommunication providers and the like.

Copyright and data protection are related subjects. They could be defined almost identically:

- Copyright: the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information created by them is communicated to others.
- Informational privacy: the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others (Westin 1967).

Therefore, there has to be a connection between these two subjects. However, there are some conflicts of interest as well. To name a few:

- the conflict between complete control of copyright on protected works on the one hand and the freedom to be let alone in the private sphere on the other;
- a conflict in the field of data protection between the United States and the European Union: the USA is even considering a procedure before the World Trade Organisation to attack the far-reaching EU Data Protection Directive (DPD).

There are three aspects of privacy that need to be taken into consideration:

1. privacy of transactional (licensing) and non-transactional (browsing) communications;
2. privacy of the home – home taping as an infringement;
3. informational privacy – protection against the processing of personal data of purchaser and/or browser.

Issues that need to be addressed include the transborder flow of personal information and the question of how to regulate the relation between copyright and data protection or copyright and privacy. Systems of self-regulation need also to be considered.

7.1 Theme 1 – Copyright versus Privacy

Copyright tends to move towards granting a right to control the use or “consumption” of information products. Should the scope of copyright overlap the users’ private sphere in this regard? Do the copyright holders’ interests justify that copyright enters the individual end-users’ private sphere? If so, should copyright holders be allowed to monitor private uses of copyrighted works through ECMSs? Is the rationale for the limitations of copyright that kept copyright outside the users’ private sphere purely of an economic and practical nature, or are privacy concerns involved here as well?

Privacy in transactions concerning information products may be viewed as closely related to the freedoms of information, expression and of association. Should, therefore, more stringent regulations be applicable to the processing of data concerning the “consumption” of information products?

Introduction by Kamiel Koelman

Up until now, copyright-holders did not enforce their copyright against private individual users, firstly, because copyright only grants a right to exercise control at the exploitation level and, secondly, because the copyright-holder could not rely on a contractual obligation. This will change through the emergence of ECMSs. These systems allow

licensing, detection of infringement or non-compliance and enforcement of copyright. Thus, the reach of copyright has expanded.

Several reasons to leave out copyright from the private sphere can be distinguished:

- economic reasons – private use was not considered economically significant;
- a choice of principle – the decision to leave the end-user's right to privacy outside the sphere of the copyright-holder could be based on its connection with rights of freedom of information and expression and the right of association.

In the digital environment of the European software and database regimes, privacy concerns do not seem to be of major importance. Both provide for a broad right of reproduction that expressly covers temporary reproductions. The copyright-holder has a legal action against an unlawful private user or acquirer of a copyrighted software or database product. In the proposed directive on copyright and related rights in the information society, a similar approach is proposed, with one remarkable difference: temporary reproductions with the sole purpose of enabling use of copyrighted works must be exempted in the national laws of the EU Member States, except when these temporary reproductions have economic significance.

All these regimes concerning electronic works expand the copyright-holder's reach. Obviously, however, enforcing copyright at the level of the individual user and especially monitoring private use of copyrighted works, could have implications for privacy.

The main issues in need of consideration are:

1. Should the balance that existed in the analogue world be upheld in a digital environment?
2. Should user privacy be taken into account when establishing the scope and limitations of copyright?
3. Should the issue of user privacy be addressed when implementing legal protection schemes to protect technological measures that safeguard copyrighted works?
4. Do the existing privacy and data protection laws protect user privacy sufficiently in the context of enforcing copyrights?

Reaction by Lucie Guibault

Copyright law has traditionally made a distinction between exploitation of a work for commercial purposes and consumption of a work for personal purposes. The private use exemption was therefore created on the basis that a non-commercial use of a work for personal purposes does not affect the interests of the copyright-holder and that copyright does not extend to an individual's private sphere. To subject the private enjoyment of works of authorship to the copyright-holder's surveillance would be an invasion of the user's autonomy and concomitantly a violation of his/her fundamental right to privacy.

With regard to home taping, which does have economic consequences for copyright-holders, it was decided that the latter should be compensated but they should not be allowed to monitor the use made of their works in the private sphere. The non-voluntary license schemes introduced here not only served to cure a market failure, but also to preserve the user's fundamental right to privacy. Today, through the implementation of

technological measures which allow copyright-holders to license directly with consumers for the use of their works, the symptoms of market failure may have essentially disappeared in the digital networked environment. Nevertheless these technological measures may still have a negative impact on the user's fundamental right to privacy. The threat is felt both on the extent to which users may make use of copyrighted material in the private sphere and on the monitoring of such use through the collection and storage of the users' personal data.

Whether a private use exemption should be recognised in the digital networked environment is a complex issue. The key element in the discussion is: what constitutes a normal exploitation of a work in the digital networked environment? Are rights-holders entitled to receive compensation for all types of private uses of lawfully obtained copies of works, just because they have the technical means to do so? As shown in the Computer Programs and Database Directives where any private use exemption is expressly excluded, the current tendency in Europe with respect to the digital environment is essentially to expand the reproduction right into a right to control the use of works.

The implementation of the provisions found in the new WIPO Treaties on technological measures and the protection of copyright management information may have an impact on the user's informational privacy because of the need to monitor the use of copyrighted material. Moreover, not all acts of circumvention of a technical device designed to protect the copyrights of the owner should be sanctioned. Acts of circumvention accomplished within the scope of statutory limitations, such as the private use exemption, should not be condemned. The monitoring of the use of copyrighted material may also entail the collection of sensitive user information. If collecting societies come to play a role in the chain of payment of royalties for the digital use of works included in their repertoire, then somewhere along the line, someone will have to collect such information as the title of the work, the number of times it has been used, who used it, etc. The manner in which this information is collected and used may have a very damaging impact on the user and will therefore have a chilling effect on consumers. Knowing that someone is monitoring what one reads, views or listens to may discourage users from consuming works altogether.

A careful and explicit balancing of interests should be conducted to determine the extent to which the user's right to privacy may be disturbed to enforce copyrights through an ECMS.

DISCUSSION

Private-public distinction

Can the distinction between private and public be maintained any longer?

In *Niemitz v Federal Republic of Germany*,¹⁸⁸ the European Court of Human Rights held that the right to privacy in Art 8 of the European Convention on Human Rights (ECHR) has to be read very broadly such that it in fact embraces the sphere outside the private home. This and a number of other decisions seem to indicate that the private-public

¹⁸⁸ (1992) A 252-B, para 29.

distinction is, at least for the purposes of Art 8, increasingly irrelevant. However, there is a very clear line in the Niemitz case which suggests that the protection of privacy is given to the human factor and to the home more than to the office. One participant adds that in the framework of Art 10 of the ECHR, the Court in Strasbourg has recognised the freedom of speech for corporations and other legal persons. Despite the fact that corporations do not have emotions and “personal” expressions, their right to public speech has been recognised. So would not the same apply in the framework of Art 8?

It is suggested by one of the participants that as soon as one enters the market and offers or communicates information to the public, one loses one’s claim to privacy. The central issue in copyright is communication to the public; reproduction is merely a preparation for this communication. As soon as one starts to communicate information, one falls under the scope of copyright. If one is consuming information, even if it is done at work but for one’s own private use, then that should not be covered by copyright at all. Under this approach, a distinction is drawn between private activities as being consumptive and public activities as being productive. It is contested, however, that this production-consumption distinction is not necessarily very clear-cut. Another participant observes that the public-private distinction is closely related to the distinction between exploiting a work and not exploiting a work. What is called public in copyright law actually comes down to exploiting a work.

One of the salient issues of the information society is how citizens are going to interact publicly and how they are going to interact privately. A solution would be that when one receives information, this is considered private and when one offers it for sale, this is considered public. The example of caller identification is given: on the one hand, the person making the call is protected from having his or her telephone number accessed; on the other hand, the person receiving the call wants to know who is invading his/her privacy at home.

The public-private distinction also comes up in another way: corporations often act for individuals, either through the assignment of rights or through other means. Performers have a privacy interest in not having their live performances recorded in permanent form until it is the version they prefer, and that is often exercised through corporations that have acquired that right through assignment. A lot of leeway exists in which to look beyond the corporate structure to see what interest is being advanced or protected.

There is a shift in society where more and more people become homeworkers, being loosely attached to companies. They use the same tool, their computer, for both private and business purposes. There might be connections made which will not be appreciated from a privacy point-of-view.

Small businesses

Do privacy concerns also relate to the privacy of small businesses or is the discussion limited to consumers – ie, individuals who do not use the information in a commercial manner? In the report, a certain distinction is made between non-commercial end-use and more commercial use that supposedly would be outside the privacy sphere. Where do we draw the line? This also comes back to the question of what is public and what is private.

The issue of privacy and data protection for legal entities, in addition to individual, natural/physical persons is very debated. In the data protection field, the usual attitude is that a legal person does not have a right to data protection because a legal person has no right to privacy. It is often claimed that the privacy concept and the values that privacy protects are only thinkable for persons with emotions. However, if we look at the definitions of privacy, we see that most of them are in fact personality-neutral. They can quite easily apply to corporate entities as well as to individual, natural/physical persons, and there seems to be no reason why data on legal entities could not be protected. Until now, however, there is no decision of the European Court of Human Rights holding that a legal entity definitely has a right to privacy as protected by Art 8 of the ECHR. There are a couple of decisions of the European Commission for Human Rights which would indicate that at least a small legal entity does have a right to privacy under Art 8. The DPD does not provide for such protection. The conclusion then might be that even commercial private use could have this extra layer of protection under the ECHR and that, of course, would have implications for copyright.

Moral rights

In European copyright law, the question whether copyright should be limited by privacy is complicated by the existence of moral rights, which confer on the author of a work a right to control the use of the work. In the USA, moral rights are recognised only to a limited degree.

In Europe, the question seems to be framed in terms of the privacy of the user versus the moral rights of the copyright-holder, whereas, in the USA, it seems to be framed in terms of the fair use rights of the user versus the freedom of contract rights of the copyright-holder. The question, however, is the same and should be resolved by reference to what constitutes normal exploitation of the work. If the “normal exploitation” of the work is to be defined as anything that can yield economic return, a privacy problem arises. The scope of copyright as an economic matter needs to be discussed to decide whether there is such a privacy problem, under both US and European law. It is countered that privacy is not less of a concern in the USA, but that the starting point is different and questions of private use exemptions will be answered differently – eg, the question of whether shrink-wrap licenses are enforceable.

One participant argues that, in the European context, moral rights may be a factor in this particular discussion, but not a dominant one. What is more important is the scope of the exploitation right, which, in most European copyright systems, is distinct from the moral right.

One participant wants to go a step further and try to avoid the issue of moral rights altogether. The most important issue here is the conflict between the economic interests of the producers of commercially exploitable information and the individual users. Information producers wish to be paid for each and every use (pay-per-use), whereas information users wish to keep their private sphere intact and be able to consume the information anonymously.

Private use exemption

An important assumption underlies the exemption for private use; this is that private use is not commercial use. Does the question whether private use exemptions should be recognised in a digital environment come out of a particular perspective of continental Europe? According to one of the participants, we must be aware that, even in the “analogue” environment, a private use exemption does not exist in many countries. However, it is countered that the private use exemption is incorporated in the fair dealing or fair use exemption in common-law countries.

Copyright – balancing interests

There are basic differences in philosophy in arguing the case for copyright. According to one participant, there seems to be a consensus that copyright is constructed as an exclusive right with exceptions. But other constructions are also possible. Both the exclusive right of the copyright-holder and the public’s right of access to the work are justified, and they are both equal in their legal basis. Therefore, a balance needs to be struck. Obviously, when the technological context changes, the balance needs to be struck again, but all the time it should be kept in mind that the primary objective is not to protect the copyright-holder. The primary objective is to balance both competing interests.

Is it possible to discuss the economic aspects of privacy protection, which is usually perceived as mostly a moral (ethical) right? There have been attempts to define the right to privacy in very harsh economic terms: one owns one’s data and if someone wants to use them for marketing purposes payment should be made. Perhaps this economic approach is helpful in our attempts to balance these competing interests. One of the participants challenges the notion of privacy as a property right. Attributing property rights to information as such is disputed. Some privacy advocates have started to embrace a market approach, proposing a regime whereby someone who uses information on a person, pays that person royalties. However, these advocates are not necessarily embracing the idea that every person, every data subject has an ownership right or a property right to data on him-/herself, but such a regime is a way of making people who process data on others think twice before doing so, as there are going to be economic implications from what they do with those data.

When striking a balance in a digital environment, should the existing balance be preserved as much as possible or should the balance be defined in a new way? Should we aim at one streamlined system or solution or should we try to develop different solutions, different ways of thinking for distinct categories of situations where, for example, cultural interests could be developed and protected along their own particular lines?

What approach should be taken when trying to balance copyright and privacy? Should we adopt a low-level approach, addressing privacy concerns under data protection laws, or by applying technology to duly protect an end-user against certain privacy-invasive practices? Or should we go one step further and recognise, in principle, that the scope of copyright is limited by privacy considerations? Under the second, more principled approach, applying all sorts of privacy-enhancing technologies would not be enough. One would have to say as a matter of principle: this is where the right stops.

According to one of the participants, privacy is not an absolute right. In the end, both copyright and privacy need to be balanced in a rather pragmatic way. Privacy and copyright are equally matched, in the sense that they can both be viewed as property rights, as personality rights or as connected to the freedom of information.

ECMSs

One of the participants doubts whether ECMSs will solve the copyright-privacy dilemma. It is suggested that practical solutions should be considered. The collective management of rights, for example, is a form of exercising rights which infringes less on privacy rights than the full exclusive right, because when exercising a right in a collective way, blanket licensing that is blind to the quantum of usage can be introduced. One participant adds that asking for every penny for every single individual use of every individual document can indeed be avoided by a subscription-oriented business model. That would be less privacy-invasive than an ECMS. Nevertheless, one can ask whether a general subscription system does not raise privacy concerns as well. Consumers pay for things they do privately in their home and although the individual use is not being controlled, it still has an impact upon the private sphere.

7.2 Theme 2 – Data Protection in Electronic Transactions

What sort of processing of purchaser-related data should be regarded as “necessary” for the purposes of entering into and monitoring compliance with a contract between a Media Distributor and a purchaser of copyrighted products? How is the notion of “legal obligation” in Art 7(c) of the EU DPD to be understood? Under what circumstances will the use of cookies mechanisms be justified? In what circumstances will ECMS operations involve processing of especially sensitive data as listed, for example, in Art 8(1) of the Directive? To what extent do data protection laws make mandatory the adoption of anonymisation techniques in the context of ECMS operations? How are we to interpret the criterion of “compatibility” in the purpose specification principle of data protection laws? To what degree can the derogations in Arts 9 and 13 of the Directive be used to permit processing of personal data otherwise not allowed under the other provisions of the Directive?

Introduction by Lee Bygrave

Data protection law is the main legal point of departure in the analysis of the implications of ECMS operations (see chapters 2–4). Due to the fact that the ambit of data protection legislation varies considerably from jurisdiction to jurisdiction, the report focuses on the DPD. It also looks to the ECHR, and the case law from the Strasbourg organs based on Art 8 of the Convention. Article 8 is very important from a normative perspective for the interpretation of the Directive. This is especially true with regard to the interpretation of the term “necessary”, which is found several times in the Directive. Case law pursuant to Art 8 suggests that the necessity criterion in the Directive should be read as involving two sub-criteria: the existence of a pressing social or commercial need, and a proportionality between ends and means.

Data protection legislation focuses on the processing of personal data. These are data from which a specific individual can be identified. What is important here is determining the extent to which ECMS operations will involve the processing of such data. This issue needs to be assessed in the light of cookie mechanisms. Another issue is which parties constitute “data controllers” in an ECMS. The Directive implies that there can be several controllers in relation to one processing operation. Furthermore, the Directive operates from the principle that one cannot process personal data unless the processing falls under a number of exemptions. The exemptions drawn up in Arts 7 and 8 of the Directive are so broad that there can be little doubt that ECMS operations fall under one, if not several, of these exemptions.

The Directive does not embrace the principle of anonymity expressly. However, this principle could be read into various provisions. Furthermore, it could follow from the necessity criterion. The extent of anonymity varies in practice. If there is full anonymity, the DPD and other laws on data protection do not apply. If there is anything less than full anonymity, the legislation could and should apply. It is often assumed that privacy-enhancing technologies (PETs) will lead to full anonymity. However, this is often not the case. For example, many forms of digital cash provide for pseudonymity in the transaction payment and not for full anonymity.

Another issue is that of secondary use of data that have been registered or processed. This issue is important in terms of how much marketing and cross-selling can be allowed. The point of departure in this context is the principle of purpose specification, often called the principle of finality also. This principle essentially stipulates that all personal data shall be processed for certain, specified and legitimate purposes and any processing of the data for other purposes will ordinarily be disallowed, unless there is some sort of compatibility between the secondary and primary purposes. The correct interpretation of compatibility in this context needs to be found.

The DPD also sets out measures on what sort of information data subjects must be given when data on them are processed. This has important implications for the issue of data subject consent.

Furthermore, the Directive makes it mandatory for EU Member States to prohibit the transfer of personal data to third countries, insofar as the third country does not provide an adequate level of protection. However, there are many exemptions to this rule on adequacy. It is probable that ECMS operations will fall under one or more of these exemptions.

DISCUSSION

General

The best way to protect data would be not to process data at all. However, because data processing will occur and it will be necessary to control copyrights, the best solution would be to anonymise data. If this is not possible, PETs or other technological mechanisms should be used to protect data in an adequate way. Some of the participants

are doubtful about the effective implementation of the Directive in the copyright field and wonder whether it might not be better to develop different data protection rules in the field of copyright.

With regard to the implementation of the Directive, the new Swedish data protection legislation follows the Directive's provisions very closely. However, many Swedes have been disappointed by the Directive. This disappointment is shared by a number of participants because the Directive is not as progressive or forward-looking as they had hoped and leaves many aspects of the new digital world untouched.

The Directive is an internal market directive: highest priority has been given, therefore, to the free flow of data in and between EU Member States and not to data protection. In order to guarantee free flow of data and electronic services, it is essential to harmonise conditions for data processing at the national level. The Directive provides for a minimum level of protection. Member states are free, therefore, to achieve a higher level of protection than provided for in the Directive. However, this could ultimately limit the free flow of personal data within the internal market.

Data Protection in ECMSs

There are many questions as to what data are indispensable for an ECMS to work. The only data which will be undoubtedly essential are certain data on the purchaser. Onward flows of data would be part of a scheme entailing the use of subscribed techniques for the onward distribution of a purchased object by a consumer in a cryptographic envelope. Theoretically, the data would go back to the copyright-holder. Consumers will need data to protect them from accusations of stealing. However, a consumer would only lose anonymity if he were to exploit information illegally.

Necessity criterion and ease/probability of identification

The participants do not see any difficulties in defining such criteria in a general way.

The notion of “collecting society”

Companies are collecting huge amounts of data. Nobody knows what should be stored nor do consumers know in which way the data will be used. It is claimed that a “collecting society” is emerging on the side of copyright-holders. One participant compared the collection of data with the collection of electronic footprints (date, time, place of call) in the telecommunications industry. The telecommunication-operators' billing systems have been developed on the basis of these footprints. It is feasible that ECMS operations will also gather these kinds of footprints.

7.3 Theme 3 – Do PETs make a difference?

If digital cash would exist, it would not be necessary to know the purchaser to receive compensation for providing a service. Would it then, in general, not be “necessary” to know the purchaser’s identity? Would the same go for works licensed through an ECMS? Would it be enough for a copyright holder to know the pseudonym of the acquirer of a

license? Should the use of digital pseudonyms or identity protectors be mandatory? If so, under what circumstances?

Should PETs, and the consequences of the application of PETs, be regulated specifically to clarify that data protection regulations do not apply, or under which circumstances they would not be applicable? Should the circumstances in which a Certification Authority may reveal a true identity be specifically regulated? Should the latter be left to market forces?

Introduction by Erik Luijck (technical)

In 1994, the Dutch Data Protection Commissioner asked us to look at privacy-enhancing technologies. At the time, the focus was on services and how consumer privacy could be protected from outside services, as it is necessary for the consumer to perform transactions without revealing his/her true identity. Therefore, it was essential to determine where identity protectors could be placed. The first solution would be to have a trusted service provider that has an identity protector for services on the Internet or an outside domain. Another solution would be to place an identity protector within the personal system. At the time, the identity protector was theoretical. However, it is now in place in certain hospital databases. It works in such a way that doctors can only access a patient's medical files and not, for example, the patient's financial files.

At present, intelligent agents are being configured. These so-called "electronic butlers" know certain things about your personal identity – they carry within them your personal data. Furthermore, an intelligent agent has the ability to learn about your reactions and by so doing can improve its service. For example, to find the most convenient and cost-effective information, it can clone itself in order to find the best solution in the shortest amount of time. To safeguard against hackers, PET-layers were added to the software. The technical part is finished. The legal implications are still being worked out.

Introduction by Michael Fromkin (legal)

In the USA, the approach to the legal aspects of PETs with regard to copyright is very different from the European approach. Presently, the USA is in the shadow of new legislation: Art 2B of the Uniform Commercial Code. These law reform activities are aimed at reducing user rights, not increasing them. However, due to the extraterritorial effects of the EU DPD, new developments could occur. Furthermore, public trust in the institutions in the USA is less than is the norm in Europe. On the other hand, the USA has some potential for extending privacy protection under the Constitution.

It is very early days for PETs. The best approach at present would be to make distinctions and identify problems. One useful distinction is between systems in which the user must disclose information, as opposed to those in which the user is not required to disclose any information. An absolute form would be not to supply information: if disclosure needs to be done, do it at home.

Another distinction is how transparent the data are. For example, cookies are not necessarily so bad, since the cookie remains on the user's computer and can be erased by the user. The issue here is not whether a cookie is given, but rather whether the user is

notified as to the content of the cookie, and, most especially, whether the cookie is transparent or not. If the cookie is incomprehensible information on the user's hard drive, there is no way for the user to monitor what the cookie really is. This issue of transparency should be addressed by consumer organisations.

Another important fact to consider about PETs is that consumers are likely to be subject to a particular form of myopia. A rational consumer with a short-term horizon will tend to value an individual datum at its marginal value, which will be lower than the average value of a group of data brought together into a database. Thus, we might reasonably expect rational consumers to continue to undervalue their privacy. Providing PETs becomes particularly important in such a scenario.

The report suggests there is an opposition between technology and privacy. However, there are actually three elements in a triangular relationship. The three elements are technology, privacy and economic efficiency/the economic rights of copyright-holders. It is quite easy to get two sides of the triangle but it seems difficult to get all three.

There are relatively few occasions in which a legal right to be anonymous occurs. There can be a moral/public policy ground for anonymity. For example, tax form requests from the government should not be a reason for opening a tax investigation.

Consequently, concern should be felt with regard to the concepts of consent in the DPD and the exception for the "enforcement of legal rights". Care has to be taken that they do not become exceptions that simply swallow the rules.

Finally, because this is such early days in the development of PETs and because the technologies are changing so quickly, there is an enormous danger of writing legal rules which assume existence of a technology that may soon be left behind. Another possible danger is the paucity of quality control of the standard setting that is occurring. This lack of control creates a risk that certain privacy-enhancing mechanisms are locked out of new technological and organisational platforms.

DISCUSSION

General

PETs are not necessarily going to take data processing out of the ambit of data protection legislation unless full anonymity applies. Whether this level of anonymity is achieved will depend on the ease or probability that is needed for identification of a person.

There is probably a legal obligation, pursuant to the DPD, to develop PETs. The use of PETs could have implications for the acts of interest balancing required by the DPD.

The data for giving licenses in the copyright field are sometimes based on the user, other times on the use. The copyright-holder would only need to know the identity of the purchaser if the copyright is infringed. To protect against fake users, use could be retracted or authorised certificates could be issued. However, it could be advantageous for the purchaser to give up his identity and become an 'infringing' seller.

It is too early to comment on the exact extent to which ECMSs will need to process personal data. One can distinguish, nevertheless, between two kinds of personal data that are required to issue, for example, a license: data that are necessary and data that are convenient. All the same, one thing is to allow processing to occur in the first place, but there are also many issues concerning the conditions of data processing.

Pseudonyms

It could be possible that each time a person begins a transaction a new pseudonym is used. It is envisaged that ECMSs could allow this.

Trusted third parties and/or Certification Authorities will be the way forward in Europe; for the USA, this is not as certain. Assuming the trusted third party can be trusted, they would know the true identity of a person and have the ability to link that identity to the pseudonym. The trusted party would also have to manage for the possibility that several pseudonyms are used simultaneously.

Many problems could be solved if there was only one information provider, one trusted third party, one set of rules. However, the aim for a perfect virtual world will limit variety and competition. The least worse system should prevail. All the same, there is a need to reach agreements on an international level to guard against imperfections, such as tax evasion.

Consent

A provider has an obligation not to do certain things unless it has the consumer's consent. However, there may be data (eg, genetic data) that a consumer cannot validly consent to processing. The relevant case law pursuant to Art 8 of the ECHR has only involved non-consensual data processing. In the future, the Court may find fundamental interests infringed even if consent is present. The DPD opens up several possibilities for data controllers to rely on data subject consent in order to process data lawfully. These possibilities may well be exploited in a manner that undermines privacy over the long term.

Consumer interest groups

Consumer interest groups will need to participate in the preliminary, standard license-making procedures for ECMS operations. At the same time, it is recognised that consumer protection interests do not always harmonise with data protection interests.

Abbreviations

A: Publications of the European Court of Human Rights, Series A – Judgements and Decisions

CDP: Copyright Directive Proposal

DPD: Data Protection Directive

ECHR: European Convention on Human Rights

ECMS: Electronic Copyright Management System

IP: Internet protocol

IPR: Intellectual property rights

ISDN: Integrated Services Digital Network

RMI: Rights Management Information

URL: Uniform Resource Locator

Bibliography

Bell 1998 = T W Bell, “Fair Use vs. Fared Use: The Impact of Automated Rights Management on Copyright’s Fair Use Doctrine”, *76 North Carolina Law Review* (1998), 557–619.

Bennett 1992 = C J Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Ithaca/London: Cornell University Press, 1992).

Bernstein & Clarida 1996 = R J Bernstein & R W Clarida, “Is Contract Pre-Emption Dead After ‘ProCD’?”, available at URL <http://www.ljextra.com/copyright/ProCD.html>.

Burkert 1997a = H Burkert, “Privacy-Enhancing Technologies: Typology, Critique, Vision”, in P E Agre & M Rotenberg (eds), *Technology and Privacy: The New Landscape* (Cambridge, Massachusetts/London: MIT Press, 1997), 125–142.

Burkert 1997b = H Burkert, “Privacy Enhancing Technologies and Trust in the Information Society”, available at URL <http://www.gmd.de/People/Herbert.Burkert/Stresa.html>.

Bygrave 1998a = L A Bygrave, “Data Protection Law: Approaching its Rationale, Logic and Limits”, doctoral thesis on file with author.

Bygrave 1998b = L A Bygrave, “Data Protection Pursuant to the Right to Privacy in Human Rights Treaties”, *6 International Journal of Law and Information Technology* (1998) – forthcoming.

Canadian Association of Internet Providers 1997 = Canadian Association of Internet Providers, *Code of Conduct*, available at URL <http://caip.ca/caipcode.htm>.

Canadian Task Force on Electronic Commerce 1998 = Industry Canada & Justice Canada, Task Force on Electronic Commerce, *The Protection of Personal Information: Building Canada's Information Economy and Society* (Ottawa: Industry Canada/Justice Canada, 1998); also available at URL <http://strategis.ic.gc.ca/privacy>.

CDB Infotek *et al* 1997 = CDB Infotek, Database Technologies Inc, Experian, First Data InfosourceDonnelly Marketing, Information America, IRSC Inc, LEXIS-NEXIS & Metromail Corp, *Individual Reference Services Industry Principles*, 10.6.1997, available at URL <http://zeus.bna.com/e-law/docs/dbguide.html>.

Clapham 1993 = A Clapham, *Human Rights in the Private Sphere* (Oxford: Clarendon Press, 1993).

Clark 1996 = C Clark, "The Answer to the Machine is in the Machine", in P B Hugenholtz (ed), *The Future of Copyright in a Digital Environment* (The Hague/London/Boston: Kluwer, 1996), 139–148.

Clarke 1996 = R Clarke, "Identification, Anonymity and Pseudonymity in Consumer Transactions: A Vital Systems Design and Public Policy Issue", version of 13.10.1996, available at URL <http://www.anu.edu.au/people/Roger.Clarke/DV/AnonPsPol.html>.

Cohen 1996 = J E Cohen, "A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace", available at URL http://38.222.224.75/sol3/paper.taf?ABSTRACT_ID=17990.

Cohen 1997 = J E Cohen, "Some Reflections on Copyright Management Systems and Laws Designed to Protect Them", 12 *Berkeley Technology Law Journal* (1997), 161–187.

Data Protection Working Party 1997a = Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, *First Orientations on Transfers of Personal Data to Third Countries: Possible Ways Forward in Assessing Adequacy*, Discussion Document adopted 26.6.1997, available at URL <http://europa.eu.int/comm/dg15/en/media/dataprot/third.htm>.

Data Protection Working Party 1997b = Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, *Anonymity on the Internet*, Recommendation 3/97 adopted 3.12.1997, available at URL <http://europa.eu.int/comm/dg15/en/media/dataprot/wp6.htm>.

Data Protection Working Party 1998 = Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, *Judging industry self-regulation: when does it make a meaningful contribution to the level of data protection in a third country?*, Working Document adopted 14.1.1998, available at URL <http://europa.eu.int/comm/dg15/en/media/dataprot/wp7.htm>.

Davies 1984 = G Davies, *Private Copying of Sound and Audio-Visual Recordings* (Oxford: ESC Publishing Ltd, 1984).

Elkin-Koren 1997 = N Elkin-Koren, “Copyright Policy and the Limits of Freedom of Contract”, 12 *Berkeley Technology Law Journal* (1997), 93–114.

Ellger 1991 = R Ellger, “Datenschutzgesetz und europäischer Binnenmarkt (Teil 2)” *Recht der Datenverarbeitung* (1991), 121–135.

European Commission 1992 = Commission of the European Communities, Amended Proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data (COM(92) 422 final – SYN 287, 15.10.1992).

European Commission 1995 = Commission of the European Communities, *Green Paper on Copyright and Related Rights in the Information Society* (COM (95) 382 final, 19.7.1995).

Ficsor 1997 = M Ficsor, “The Spring 1997 Horace S. Manges Lecture – Copyright for the Digital Era: The WIPO “Internet” Treaties”, 21 *Columbia VLA Journal of Law & the Arts* (1997), 197–224.

Froomkin 1996 = M Froomkin, “Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases”, 15 *University of Pittsburg Journal of Law and Commerce* (1996), 395ff; also available at URL <http://www.law.miami.edu/~froomkin/articles/oceanno.html>.

Froomkin 1997 = M Froomkin, “The Internet as a Source of Regulatory Arbitrage”, in B Kahin & C Nesson (eds), *Borders in Cyberspace: Information Policy and the Global Information Infrastructure* (Cambridge, Massachusetts/London: MIT Press, 1997), 129–163; also available at URL <http://www.law.miami.edu/~froomkin/articles/arbitr.html>.

Gavison 1980 = R Gavison, “Privacy and the Limits of Law” 89 *Yale Law Journal* (1980), 421–471.

Geller 1996 = P E Geller, “Conflicts of Law in Cyberspace: International Copyright in a Digitally Networked World”, in P B Hugenholtz (ed), *The Future of Copyright in a Digital Environment* (The Hague/London/Boston: Kluwer, 1996), 27–48.

Goldberg, Wagner & Brewer 1997.= I Goldberg, D Wagner & E Brewer, “Privacy-enhancing technologies for the Internet”, available at URL <http://www.cs.berkeley.edu/~daw/privacy-compcon97-www/privacy-html.html>.

Greenleaf 1995 = G Greenleaf, “European Privacy Directive and data exports” 2 *Privacy Law & Policy Reporter* (1995), 105–108.

Greenleaf 1996a = G Greenleaf, “Privacy and cyberspace – an ambiguous relationship” 3 *Privacy Law & Policy Reporter* (1996) 88–92.

- Greenleaf 1996b = G Greenleaf, “Privacy principles – irrelevant to cyberspace?” 3 *Privacy Law & Policy Reporter* (1996), 114–119.
- Haeck 1998 = J F Haeck, *Idee en Programmaformule in het Auteursrecht* (Deventer: Kluwer, 1998).
- Haeger 1962 = S Haeger, “Die Einbruch von Nutzungsrechten in die Privatsphäre”, 37 *Archiv für Urheber- Film- Funk- und Theaterrecht* (1962), 45–72.
- Harris *et al* 1995 = D J Harris, M O’Boyle & C Warbrick, *Law of the European Convention on Human Rights* (London/Dublin/Edinburgh: Butterworths, 1995).
- Hefermehl 1957 = W Hefermehl, “Magnetton-Aufnahmen urheberrechtlich geschützter Werke zum persönlichen Gebrauch”, 24 *Archiv für Urheber- Film- Funk- und Theaterrecht* (1957), 56–92.
- Hugenholtz 1996a = P B Hugenholtz, “Adapting Copyright to the Information Superhighway”, in P B Hugenholtz (ed), *The Future of Copyright in a Digital Environment* (The Hague/London/Boston: Kluwer, 1996), 81–102.
- Hugenholtz 1996b = P B Hugenholtz, “De Databankrichtlijn eindelijk aanvaard, een zeer kritisch commentaar”, *Computerrecht* (1996), 131–137.
- Hughes 1988 = J Hughes, “The Philosophy of Intellectual Property”, 77 *The Georgetown Law Journal* (1988), 287–366.
- Information Infrastructure Task Force 1995 = Information Infrastructure Task Force, Privacy Working Group, *Principles for Providing and Using Personal Information*, adopted 6.6.1995, available at URL gopher://ntiant1.ntia.doc.gov:70/h0/papers/documents/files/niiprivrin_final.html.
- Institute for Information Law 1997a = Institute for Information Law (L Guibault), *Contracts and Copyright Exemptions* (Amsterdam: Institute for Information Law, 1997).
- Institute for Information Law 1997b = Institute for Information Law (K J Koelman), *Liability for On-Line Intermediaries* (Amsterdam: Institute for Information Law, 1997).
- ICC 1998 = ICC, *Revised Guidelines on Advertising and Marketing on the Internet*, adopted 2.4.1998, available at URL http://www.iccwbo.org/Comm/html/Internet_Guidelines.html.
- International Working Group on Data Protection and Telecommunications 1996 = International Working Group on Data Protection and Telecommunications, *Budapest-Berlin Memorandum on Data Protection and Privacy on the Internet*, adopted 19.11.1996, available at URL http://www.datenschutz-berlin.de/diskus/13_15.htm.

LAB 1995 = Legal Advisory Board for the Information Market, *Reply to the Green Paper on Copyright and Related Rights in the Information Society* (1995), available at URL <http://guagua.echo.lu/legal/en/ipr/reply/reply.html>

Litman 1997a = J Litman, "Symposium: Copyright Owners' Rights and Users' Privileges on the Internet: Reforming Information Law in Copyright's Image", 22 *Dayton Law Review* (1997), 587–619.

Litman 1997b = J Litman, "New Copyright Paradigms", available at URL <http://www.msen.com/~litman/paradigm.htm>.

Lucas 1997 = A Lucas, "Copyright Law and Technical Protection Devices", 21 *Columbia VLA Journal of Law & the Arts* (1997), 225–238.

Mackaay 1996 = E Mackaay, "The Economics of Emergent Property Rights on the Internet", in P B Hugenholtz (ed), *The Future of Copyright in a Digital Environment* (The Hague/London/Boston: Kluwer, 1996), 13–26.

Mayer-Schönberger 1997 = V Mayer-Schönberger, "The Internet and Privacy Legislation: Cookies for a Treat?" 1 *West Virginia Journal of Law and Technology* (1997), no 1, available at URL <http://www.wvjolt.wvu.edu/issue1/articles/mayer/mayer.html>.

Miller 1971 = A R Miller, *The Assault on Privacy: Computers, Data Banks, and Dossiers* (Ann Arbor: University of Michigan Press, 1971).

Nicholson 1995 = B J Nicholson, "The Ghost in The Machine: Mai Systems Corp. v. Peak Computer, Inc. and the Problem of Copying in RAM", 10 *Berkeley Technology Law Journal* (1995), 147–176.

Nimmer & Nimmer = M B Nimmer & D Nimmer, *Nimmer on Copyright*, (New York/San Francisco: Mathew Bender & Co, loose leaf).

Nouwt & Vorselaars 1996 = J Nouwt & H A C M Vorselaars, "Privacy in Cyberspace", in V Bekkers, B-J Koops & S Nouwt (eds), *Emerging Electronic Highways: New Challenges for Politics and Law* (The Hague/London/Boston: Kluwer Law International, 1996), 103–120.

Olson 1992 = E W Olson, "Galoob v. Nintendo: Subject Matter Fixation and Consumer Fair Use Define the Scope of Copyright Protection for Interoperable Works", 18 *Rutgers Computer & Technology Law Journal* (1992), 879–918.

Patterson & Lindberg 1991 = L R Patterson & S W Lindberg, *The Nature of Copyright, A Law of Users' Rights* (Athens/London: The University of Georgia Press, 1991).

Proceedings of the First IMPRIMATUR Consensus Forum 1996 = Proceedings of the First IMPRIMATUR Consensus Forum (1996), available at URL <http://www.imprimatur.alcs.co.uk/download.htm>.

Ricketson 1987 = S Ricketson, *The Berne Convention for the protection of literary and artistic works: 1886–1986* (London/Reading: The Eastern Press Ltd., 1987).

Reinbothe 1981 = J Reinbothe, “Compensation for Private Taping Under Sec. 53(5) of the German Copyright Act”, *International Review of Industrial Property and Copyright Law* (1981), 36–49.

Samarajiva 1997 = R Samarajiva, “Interactivity As Though Privacy Mattered”, in P E Agre & M Rotenberg (eds), *Technology and Privacy: The New Landscape* (Cambridge, Massachusetts/London: MIT Press, 1997), 277–309.

Schoning 1998 = P Schoning, “Danish Report, In Response to François Dessemonet’s Questionnaire”, in G Roussel (ed), *Conference Proceedings of the ALAI Conference 1997* (Cowansville: Les Éditions Yvon Blais Inc, 1998), 174–180.

Schwartz 1995 = P M Schwartz, “European Data Protection Law and Restrictions on International Data Flows” 80 *Iowa Law Review* (1995), 471–496.

Spitzbarth 1963 = R Spitzbarth, “Der Streit um die private Tonbandaufnahme”, 16 *Neue juristische Wochenschrift* (1963), 881–884.

Spoor 1996 = J H Spoor, “The Copyright Approach to Copying on the Internet: (Over)Stretching the reproduction Right?”, in P B Hugenholtz (ed), *The Future of Copyright in a Digital Environment* (The Hague/London/Boston: Kluwer, 1996), 67–80.

Spoor & Verkade 1993 = J H Spoor & D W F Verkade, *Auteursrecht* (Deventer: Kluwer, 1993).

Stewart & Sandison 1989 = S M Stewart & H Sandison, *International Copyright and Neighbouring Rights* (London/Boston/Sidney: Butterworth, 1989).

Terwangne & Louveaux 1997 = C de Terwangne & S Louveaux, “Data Protection and Online Networks”, 13 *Computer Law & Security Report* (1997), 234–246.

Visser 1996 = D J G Visser, “Auteursrechtvergoedingen in Europa en de VS”, *ITeR deel 2* (Alphen aan den Rijn/Diegem: Samson Bedrijfsinformatie bv, 1996), 202–321.

Visser 1997 = D J G Visser, *Auteursrecht op toegang, De exploitatierechten van de auteur in het tijdperk van digitale informatie en netwerkcommunicatie* (The Hague: VUGA Uitgeverij BV, 1997).

Warren & Brandeis 1890 = S D Warren & L D Brandeis, “The Right to Privacy”, 4 *Harvard Law Review* (1890), 193–220.

Westin 1967 = A F Westin, *Privacy and Freedom* (New York: Atheneum, 1967).

Zimmerman 1992 = D L Zimmerman, "Information as Speech, Information as Goods: Some Thoughts on Marketplaces and the Bill of Rights", 33 *William & Mary Law Review* (1992), 665–740.